

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 7/00, 20/10, 7/26, 20/12	A1	(11) 国際公開番号 WO96/16401 (43) 国際公開日 1996年5月30日 (30.05.96)
(21) 国際出願番号 PCT/JP95/02339 (22) 国際出願日 1995年11月16日 (16.11.95) (30) 優先権データ 特願平6/283415 1994年11月17日 (17.11.94) JP 特願平7/16153 1995年2月2日 (02.02.95) JP 特願平7/261247 1995年10月9日 (09.10.95) JP (71) 出願人 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP] 〒571 大阪府門真市大字門真1006番地 Osaka, (JP) (72) 発明者 大嶋光昭 (OSHIMA, Mitsunaki) 〒615 京都府京都市西京区桂南巽町115-3 Kyoto, (JP) 後藤芳稔 (GOTOH, Yoshiho) 〒536 大阪府大阪市城東区東中浜4丁目9番17号201号室 Osaka, (JP) (74) 代理人 弁理士 松田正道 (MATSUDA, Masamichi) 〒532 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka, (JP)		(81) 指定国 CN, JP, KR, MX, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). 添付公開書類 国際調査報告書
<p>(54) Title : MARKING GENERATING APPARATUS, METHOD OF FORMING LASER MARKING ON OPTICAL DISK, REPRODUCING APPARATUS, OPTICAL DISK AND OPTICAL DISK PRODUCING METHOD</p> <p>(54) 発明の名称 マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法</p> <p>(57) Abstract</p> <p>The invention improves the duplication prevention capacity in comparison with the prior art. In the optical disk according to the present invention, for example, marking is made on a reflection film of the disk on which data are written by a laser beam, at least the position information of the marking or information on the position information is written on the disk in the form of cipher or digital signature.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>(1) ... disk factory</p> <p>(2) ... cure disk with UV</p> <p>(3) ... print label</p> <p>(5) ... synthesis</p> <p>(6) ... software</p> <p>(7) ... author software</p> <p>(8) ... extract software characteristic information</p> <p>(9) ... cipher software characteristic information</p> <p>(10) ... software characteristic information</p> <p>(11) ... original disk characteristic information</p> <p>(12) ... position information</p> <p>(13) ... laser marking</p> <p>(14) ... laser</p> <p>(15) ... marking</p> <p>(16) ... detect position information of mark</p> <p>(17) ... read address position signal of laser</p> </div> <div style="width: 45%;"> <p>(18) ... software maker</p> <p>(19) ... step 4 ciphering</p> <p>(20) ... ciphering (secret key/open key)</p> <p>(21) ... main cipher</p> <p>(22) ... laser</p> <p>(23) ... bar code</p> <p>(24) ... marking</p> <p>800 ... completion of disk</p> <p>818 ... disk production process</p> <p>817 ... secondary recording step</p> <p>818a ... input software</p> <p>818b ... produce original disk</p> <p>818c ... mold disk</p> </div> </div> <div style="margin-top: 10px;"> <p>818f ... produce first reflective film</p> <p>818i ... bonding</p> <p>818g ... mold disk</p> <p>818h ... produce second reflective film</p> <p>818a ... step 1</p> <p>818b ... step 3</p> <p>818c ... first secret key/second secret key</p> <p>818d ... step 3, write ciphered position information</p> <p>820 ... software production step</p> </div>		

(57) 要約

複製防止能力を従来に比べてより一層向上させることが出来る、マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法を提供すること。そのために、例えば本発明の光ディスクは、データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはデジタル署名された形で、前記ディスクに書き込まれている。

情報としての用途のみ

PCTに基づいて公開される国際出願をパンフレット第一頁にPCT加盟国を特定するために使用されるコード

AL	アルバニア	DK	デンマーク	LK	スリランカ	PT	ポルトガル
AM	アルメニア	DE	ドイツ	LR	リベリア	RO	ルーマニア
AT	オーストリア	EE	エストニア	LS	レソト	RU	ロシア連邦
AU	オーストラリア	ES	スペイン	LT	リトアニア	SD	スーダン
AZ	アゼルバイジャン	FI	フィンランド	LV	ラトヴィア	SE	スウェーデン
BB	バルバドス	FR	フランス	MC	モナコ	SG	シンガポール
BF	ブルキナ・ファソ	GB	イギリス	MD	モルドバ	SI	スロベニア
BG	ブルガリア	GE	グルジア	MG	マダガスカル	SK	スロバキア共和国
BJ	ベナン	GR	ギリシャ	ML	マリ	SN	セネガル
BR	ブラジル	GU	グアム	MR	モーリタニア	SZ	スワジランド
BY	ベラルーシ	IE	アイルランド	MW	モザンビーク	TD	チャド
CA	カナダ	IT	イタリア	MX	メキシコ	TG	トーゴ
CF	中央アフリカ共和国	JP	日本	NE	ニジェール	TH	タイ
CG	コンゴ	KE	ケニア	NL	オランダ	TM	トルクメニスタン
CH	スイス	KR	大韓民国	NO	ノルウェー	TR	トルコ
CI	コート・ジボワール	KZ	カザフスタン	NZ	ニュージーランド	TT	トリニダード・トバゴ
CM	カメルーン	LI	リヒテンシュタイン	PL	ポーランド	UG	ウガンダ
CN	中国					US	米国
CZ	チェコ共和国					UZ	ウズベキスタン共和国
DE	ドイツ					VN	ベトナム

明 細 書

マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法

技術分野

本発明は、たとえば、光ディスクの複製防止に利用可能な、マーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法に関するものである。

背景技術

近年、ROM型光ディスクの普及に伴い、海賊版ディスクが登場し、著作権者の権利を侵害している。

これは、ROMディスクの製造装置が容易に入手できるようになり、かつ操作が簡単になったことによる。

海賊版業者は、CDのソフトの論理データのみを抽出し、磁気テープに落とし、原盤作成装置にセットするだけで、CDの原盤ができる。この1枚の原盤をもとに数十万枚の海賊版ディスクがプレス成形できる。この場合、海賊版業者は著作権料を支払わないため安い価格で海賊版ディスクを販売し、利益を上げている。当然、この分だけ著作権者は損害を被ることになる。

今のCD規格においては、CDの論理データを読み出す機能しかなく、ディスクの物理的特徴を検出する機能をもっていない。このため論理データをビット複写によりコピーするだけで、海賊版CDが作成できる。

この物理的特徴を識別する機能を追加することにより、海賊版を防止する方法

が従来技術として知られている。

これは、原盤に物理的なマークを加える規格を新たに作ることにより、この規格のディスクの海賊版の製造を防止する。従来例として特開平5-325193に示すような海賊版防止方式が知られている。この方式はカッティング時に、意図的に特定の領域の記録時に記録ビームをトラッキング方向に走査させ、ウォブリングを原盤上に形成する。このディスクを再生する時は再生プレーヤ側で、ウォブリング検出回路を設け、このウォブリングが特定の領域にあるかどうかをチェックする。特定のウォブリング周波数のウォブリングが特定の領域にある場合は正規ディスク、ない場合は海賊版ディスクと判断する。

つまり、ウォブリング機能をもつ特殊な原盤製造装置を用いて、予め設定された物理マークの設計データに基づき、原盤にその物理マークを作成するものである。従って、海賊版業者はこの特殊な原盤製造装置も物理マークの設計データも、もっていないため、海賊版ディスクを製造できない。この場合、この規格のディスクには全て海賊版防止マークをつける必要がある。しかし、この物理マークは正規ディスクを観察することにより得られるので、この特殊な原盤製造装置を海賊版業者が入手した段階で海賊版が製造されるという問題点があった。本明細書ではこの原盤に物理マークを設けるタイプの海賊版防止方式を原盤レベル方式と呼ぶ。

他にも、この原盤レベル方式でさらに複雑な物理マークを作成する方法が提案されている。しかし、原盤レベルで如何に複雑な物理マークを作成しても、正規ディスクの樹脂を溶かして、直接全く同じ物理形状のレプリカを作成する原盤複製方法であるレプリカ方式が知られている。この方法は原盤1枚を複製するのに時間がかかり、高コストであるが、海賊版原盤1枚から数十万枚のディスクが成

形できるので、海賊版ディスク 1 枚あたりのコストは安い。従って、今後登場するレプリカ方式の普及に伴い、原盤レベルの海賊版防止技術の防止効果が無意味化するという問題点があった。

以上のように、従来の海賊版防止技術にはいくつかの課題があることがわかる。

以下、これらの課題をまとめる。

課題 1 として、従来の、原盤レベルの海賊盤防止方式の物理マークはレプリカ複製が可能なため、防止効果が低い。

課題 2 として、物理マークの設計データに基づき、物理マークを作成する従来方法では正規ディスクメーカーと同じ精度の製造装置を入手することにより、容易に海賊版を製造できる。

課題 3 として、従来の海賊盤防止方式は安全性のレベルが固定されているため、時代の経過とともに向上する海賊版技術に対して効果が低下する。

課題 4 として、防止機能のついていないディスクフォーマットとついていないディスクフォーマットの双方を認めると防止機能のついていないディスクフォーマットで海賊版ディスクが製造される。このため、全てのディスクに防止機能をつける必要があった。ゲーム規格ディスクのように閉じた規格に限定されている。

課題 5 として、従来方式では一部のライセンス親会社が特殊な製造装置をもち、公開しない。このため、各ソフトメーカーは親会社でしかディスクを製造できない。

課題 6 として、原盤マーク方式では 1 枚の原盤に対して成形されたディスクは全て同じディスク ID をもつ。つまり、1 つのパスワードで他のディスクが動作する。このため、フロッピーや通信回線を併用しないとパスワードセキュリティが保てない。また、二次記録できないため、パスワードを毎回入力する必要があった。

発明の開示

本発明は、上記従来課題を考慮し、複製防止能力を従来に比べてより一層向上させることを目的とする。

即ち、本発明では、上記の従来海賊版防止方式の6つの課題を解決するために、以下の手段を提供する。

まず、課題1に対しては、従来の原盤レベルの物理マークに代わるものとして、ディスクの反射膜に物理マークを設ける反射膜レベルの物理マークによる海賊版防止方式を提供する。これにより、原盤レベルで複製されても海賊版が防止できる。

課題2に対しては、2枚貼り合わせROMディスクにレーザーで二次記録する新しいROM記録手段を用いる。まず、第1ステップでランダムに物理マークを作成し、次に第2ステップで $0.13\mu\text{m}$ の高い測定精度で、物理マークを測定する。第3ステップでこの位置情報を暗号化して上記二次記録手段を用いてROMディスクに数十 μm 、つまり通常の加工精度でバーコード記録する。こうして通常の装置の加工精度をよりはるかに高い精度、例えば $0.1\mu\text{m}$ の光マーク位置情報が得られる。市販の加工光マークをこの $0.1\mu\text{m}$ の精度で加工することはできないため海賊版の製造は防止される。

課題3に対しては位置情報をデジタル署名暗号化した暗号として、ディスク上に安全度の低い第1世代の暗号と安全度の高い第2世代の暗号の双方を、予め記録する媒体を用いることにより、世代の異なる再生装置においてもその世代に対応した暗号の安全度で海賊版を防止する。

課題4に対してはそのソフトに対して著作権が海賊版防止機能を付与したか、

してないかを示す海賊版防止機能識別子を原盤に記録する。この識別子が改ざんされないように、原盤にソフトコンデンツを記録する際にソフトコンテンツの圧縮情報とこの海賊版防止識別子をスクランブルして暗号化して記録する。この識別子が改ざんできないため海賊版非対策ディスクフォーマットのディスクを海賊版業者が作成できない。従って海賊版の製造が防止される。

課題5に対しては、ディスク製造に不可欠なデジタル署名暗号の秘密鍵に関してマスタ鍵よりサブ鍵を生成し、各ソフトメーカにサブ鍵を渡すことにより、サブ鍵によりソフトメーカが自社の工場で正規ディスクを製造できる。

課題6に対しては、本発明のディスク毎に異なる海賊版防止マークの位置情報をディスク識別子として用いる。位置情報とディスクのシリアル番号、つまりディスクIDを合成して、デジタル署名暗号化することにより改ざんできないディスクIDを一枚毎に付与する。完成ディスク1枚毎にIDが異なるため、パスワードも異なる。従って、他のディスクでは、このパスワードは動作しないため、パスワードセキュリティが向上する。

また、本発明の二次記録により、パスワードをディスクに二次記録することによりそのディスクは永久に動作可能となる。

以上6つの課題を解決する具体的な方法を実施例を用いて以下に開示する。

本発明は、ディスクに形成された反射膜にマーキングを施すマーキング生成手段と、前記マーキングの位置を検出するマーキング位置検出手段と、前記検出された位置をマーキングの位置情報として出力する位置情報出力手段とを備えたマーキング生成装置である。

又、本発明は、少なくとも前記出力された位置情報又はその位置情報に関する情報を前記ディスクに、又は別の媒体に書き込むための位置情報書き込み手段を

備えたマーキング生成装置である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜が形成されたディスクを少なくとも1つ含む2枚のディスクを張り合わせるステップと、その張り合わされたディスクの前記反射層に対して、レーザーによりマーキングの形成を行なうステップとを備えた光ディスクのレーザーマーキング形成方法である。

又、本発明は、ディスクに形成された反射膜にマーキングを施し、前記マーキングの位置を検出し、少なくとも前記検出された位置がマーキングの位置情報として出力された、そのマーキングの位置情報又はその位置情報に関する情報を読み取る位置情報読み取り手段と、前記マーキングの現実の位置に関する情報を読み取るマーキング読み取り手段と、前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とを利用して、それらを比較判定する比較判定手段と、前記比較判定手段の比較判定結果に基づいて、前記光ディスクの記録データを再生する再生手段とを備えた再生装置である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜に対してマーキングを施すステップと、前記マーキングの位置を検出するステップと、前記検出された位置をマーキングの位置情報として出力し、暗号化して前記ディスクに書き込むステップとを備えた光ディスク製造方法である。

又、本発明は、ディスクの成形を行うステップと、前記成形されたディスクに反射膜を形成するステップと、前記反射膜に対してマーキングを施すステップと、前記マーキングの位置を検出するステップと、前記検出された位置をマーキングの位置情報として出力し、その位置情報に関連してデジタル署名して前記ディ

スクに書き込むステップとを備えた光ディスク製造方法である。

又、本発明は、データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはデジタル署名された形で、前記ディスクに書き込まれている光ディスクである。

又、本発明は、レーザーにより消滅しない材料からなる2つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザーによりマーキングが施されている光ディスクである。

図面の簡単な説明

第1図は本実施例におけるディスクの製造工程と二次記録工程図である。

第2図(a)は実施例におけるディスクの上面図、(b)は実施例におけるディスクの上面図、(c)実施例におけるディスクの上面図、(d)実施例におけるディスクの横断面図、(e)実施例における再生信号の波形図である。

第3図は本実施例における、暗号化された位置情報をディスク上にバーコードにより記録する工程のフローチャート図である。

第4図は本実施例におけるディスクの作成工程及び二次記録工程図(その1)である。

第5図は本実施例におけるディスクの作成工程及び二次記録工程図(その2)である。

第6図は本実施例における2層ディスクの作成工程図(その1)である。

第7図は本実施例における2層ディスクの作成工程図(その2)である。

第8図(a)は本実施例における張り合わせタイプの無反射部の拡大図、(b)

は本実施例における単板タイプの無反射部の拡大図である。

第9図(a)は本実施例における無反射部の再生波形図、(b)は本実施例における無反射部の再生波形図、(c)は本実施例における無反射部の再生波形図である。

第10図(a)は本実施例における張り合わせタイプの無反射部の断面図、(b)は本実施例における単板タイプの無反射部の断面図である。

第11図は本実施例における無反射部の断面を、透過電子顕微鏡により観察した結果を基にした模式図である。

第12図(a)は本実施例におけるディスクの断面図、(b)は本実施例におけるディスクの無反射部の断面図である。

第13図(a)は同実施例における正規のCDのアドレスの物理配置図、(b)は同実施例における不正に複製されたCDのアドレスの物理配置図である。

第14図は実施例におけるディスク作成とディスク作成のブロック図である。

第15図は実施例における低反射部位置検出部のブロック図である。

第16図は実施例における低反射部のアドレス・クロック位置検出の原理図である。

第17図は実施例における正規ディスクと複製ディスクの低反射部アドレス表の比較図である。

第18図は実施例における一方向関数によるディスク照合のフローチャート図である。

第19図は実施例における原盤別アドレスの座標位置の比較図である。

第20図は実施例における低反射位置検出プログラムのフローチャート図である。

第 2 1 図は同実施例の磁気記録装置のブロック図である。

第 2 2 図は同実施例における RSA 関数を用いた場合の暗号化等についてのフローチャート図である。

第 2 3 図は同実施例における楕円関数を用いた場合のデジタル署名等についてのフローチャート図である。

第 2 4 図は同実施例における位置情報の照合プロセスのフローチャート図である。

第 2 5 図は同実施例における情報処理装置のブロック図である。

第 2 6 図は同実施例における第 2 低反射部の上面図である。

第 2 7 図は本実施例における 1 層目のマーキング信号の検出波形図である。

第 2 8 図は本実施例における 2 層目のマーキング信号の検出波形図である。

第 2 9 図は本実施例におけるディスク作成装置のブロック図である。

第 3 0 図は本実施例における無反射部の符号図である。

第 3 1 図は本実施例における無反射部の検出波形図である。

第 3 2 図は本実施例におけるバーコード記録情報の内容及び相互関係の説明図である。

第 3 3 図は本実施例における二層ディスクの無反射部の斜視図である。

第 3 4 図は本実施例における流通におけるデータの流れを説明する図である。

第 3 5 図は本実施例における流通におけるディスクの流通図である。

第 3 6 図は本実施例における位置情報などをマスタ鍵とサブ鍵等を用いて、複雑に暗号化する場合の、製造過程を説明するブロック図である。

第 3 7 図は本実施例における位置情報などをマスタ鍵とサブ鍵等を用いて、複雑に暗号化する場合の、製造過程を説明するブロック図である。

第 38 図は本実施例における再生装置におけるフローチャート図である。

第 39 図は本実施例における光ディスクに秘密鍵系と公開鍵系を併用した場合の、再生装置との関係を示す図である。

第 40 図は本実施例における、光ディスクについて、位置情報などをマスタ鍵とサブ鍵等を用いて暗号化したものを記録し、再生する場合のアウトラインを示すブロック図である。

第 41 図は本実施例における光ディスクの再生装置のブロック図である。

第 42 図は本実施例のプログラムインストールにおけるスクランブル識別子の動作とドライブ ID とディスク ID の切り換えを示すフローチャート図である。

発明を実施するための最良の形態

以下、本発明にかかるマーキング生成装置、光ディスクのレーザーマーキング形成方法、再生装置、光ディスク、及び光ディスク製造方法の実施例を構成と動作を伴せて説明する。

本実施例では、先ず、前半部 (1) において、ディスクを作成すること、レーザーを利用してマーキングを作成すること、そのマーキングの位置情報を読み取ること、さらにその位置情報等を暗号化等して光ディスクに書き込むこと、そしてその光ディスクのプレーヤ側の再生動作などについて述べる。なお、その暗号化の点と再生動作に関しては簡単に述べる。

次に、後半部 (2) において、その簡単に述べられた、マーキング位置情報等の暗号化等、光ディスクの位置情報等復号再生等について詳細に説明する。又、その他の、海賊版防止に関する様々な工夫についても述べる。

なお、本明細書においては、レーザートリミングはレーザーマーキングとも呼

び、光学マーキング無反射部は単に、マーキング、あるいは光学マーキング、ディスク固有の物理ID等とも呼ぶ。

(1) 第1図は、ディスク作成工程から光ディスクの完成までの全体の大きな流れを示すフローチャートである。

まずソフト会社がソフト制作820においてソフトのオーサリングを行う。完成したソフトは、ソフト会社から、ディスク製造工場に渡される。そして、ディスク製造工場のディスク製造工程816では、ステップ818aで完成したソフトを入力して、原盤を作成し(ステップ818b)、ディスクを成形し(ステップ818e、ステップ818g)、それぞれのディスクに反射膜を作成し(ステップ818f、ステップ818h)、それら2枚のディスクを貼り合わせて(ステップ818i)、DVDやCD等のROMディスクを完成させる(ステップ818m等)。

このようにして完成したディスク800は、ソフトメーカーもしくはソフトメーカーの管理下にある工場に渡され、二次記録工程817においては、第2図に示すような、海賊版防止のマーキング584を施された後(ステップ819a)、測定手段によりこのマークの正確な位置情報を読み取り(ステップ819b)、ディスク物理特徴情報としての位置情報を得る。ステップ819cでこのディスク物理特徴情報を暗号化する。ステップ819dでは、この暗号をPWM変調した信号をレーザにより、バーコード信号としてディスク上に記録する。なおステップ819cでソフトの特徴情報とディスク物理特徴情報を合成した情報を暗号化してもよい。

さらに、上記各工程を詳しく具体的に述べる。すなわち、第4図、第5図、第8図～第12図などを用いて本発明による詳細な光ディスクのディスク作成工程

とマーキング作成工程とマーキング位置読み取り工程と暗号書き込み工程を説明する。尚、第6図、第7図を用いて、反射層が2つある場合について、補足説明を加える。また、ここでマーキング作成工程とマーキング位置読み取り工程と書き込み工程を総合して二次記録工程と呼ぶ。

(A) まず、ディスク作成工程について説明する。第4図に示すディスク作成工程806では、工程(1)で、透明基板801を成形する。工程(2)でアルミや金等の金属をスパッタリングさせ、反射層802を形成する。別の工程で作成した基板803に紫外線硬化樹脂の接着層804をスピコートにより塗布し、反射層802をもつ透明基板801と張り合わせた後、高速回転させ張り合わせ間隔を均一にさせる。外部から紫外線を照射することにより硬化し、2枚は固く接着される。工程(4)でCDやDVDのタイトルが印字された印刷層805をスクリーン印刷やオフセット印刷で印刷する。こうして、工程(4)で通常の貼り合わせ型の光ROMディスクが完成する。

(B) 次に、第4図と第5図を用いて、マーキング作成工程について説明する。第4図において、YAG等のパルスレーザー813を用いて、集束レンズ814によりレーザー光を反射層802近傍に集束させることにより、第5図の工程

(6)に示すように無反射部815を形成する。即ち、第5図の工程(6)において形成された無反射部815から工程(7)の波形(A)に示すように顕著な波形が再生される。この波形をスライスすることにより波形(B)のようなマーキング検出信号が得られ、信号(d)に示すようなアドレス、そして、信号(e)に示すようなアドレス、フレーム同期信号番号、再生クロック数の階層的なマークの位置情報が測定できる。

尚、ここで、上述したように、第6図、第7図を用いて、別のタイプのディス

ク（２層式の張り合わせディスク）について、補足説明を加える。

即ち、第４図、第５図は、反射層が片側の基板８０１にのみ形成されるいわゆる一層式の張り合わせディスクの場合を示していた。これに対して、第６図、第７図は、反射層が、基板８０１、８０３の両方に形成される、いわゆる２層式の張り合わせディスクの場合を示している。両者は、レーザトリミングを行う上で、基本的には、同じ工程（５）（６）で処理されるが、主なる相違点を簡単に説明する。まず、１層式の場合は、反射層が７０％以上の高反射率を有するアルミの膜であるのに対して、２層式の場合は、読みとり側の基板８０１に形成される反射層８０１が、３０％の反射率を有する半透過性の金（Au）の膜であり、印刷層側の基板８０３に形成される反射層８０２は、上記１層式の場合と同じものである。次に、２層式の場合は、１層式に比べて、接着層８０４が、光学的に透明であること、厚みが均一であること、レーザトリミングにより光学的な透明性を失わないこと等の光学的な精密度が要求される。又、第７図（７）、（８）、

（９）では２層の記録層のディスクの第１層の波形を示す。２層目の波形そのものは１層目の波形に比べて単に信号レベルが低いだけでさほど変わらない。しかし、１層と２層は張り合わせてあるため両者の相対位置精度はランダムであり数百ミクロンの精度でしか制御できない。後で説明するが、レーザービームは２枚の反射膜を貫通しているため、海賊版ディスクをつくるには、例えば第１マークの１層目の位置情報と２層目の位置情報を正規ディスクと同じ値に一致させる必要がある。しかし一致させるには、サブミクロンに近い張り合わせ精度が必要であるため、２層方式の海賊版ディスクの製造は事実上不可能となる。

ここで、この光学マーキング無反射部作成技術について、以下の（ａ）～（ｄ）で、張り合わせタイプと単板タイプについて、更に詳しく、第８図～第１２図等

を参照しながら説明する。第8図(a), (b)は、光学マーキング無反射部を平面的に見た場合の顕微鏡写真であり、第10図は、2層式の張り合わせディスクの無反射部の略示断面模式図である。

(a) $5\mu\text{J}$ /パルスのYAGレーザーを用いて0.6mm厚のディスクを張り合わせた合計1.2mm厚のROMディスクの0.6ミリの深さにある500オングストロームのアルミ層にレーザーを照射したところ、第8図(a)の750倍の顕微鏡写真に示すような $12\mu\text{m}$ 幅のスリット状の無反射部815が形成された。この場合、750倍の顕微鏡写真では、無反射部815には、アルミの残りカスは全く確認できなかった。無反射部815と反射部との境界部には200オングストロームの厚みで、 $2\mu\text{m}$ 幅の厚く盛り上がったアルミ層が観察できた。第10図(a)に示すように内部では大きな破損が起こっていないことを確認した。この場合、パルスレーザーの照射によりアルミの反射層が溶融し、表面張力により両側の境界部に蓄積される現象がおこっていると考えられる。我々は、これをHMST記録方式と呼ぶ(Hot Melt Surface Tention Recording Method)。この現象は貼り合わせディスク800にのみ観察される特徴的な現象である。更に、第11図に、上記レーザートリミングによる無反射部の断面を、透過電子顕微鏡(TEM)により観察した結果を基にした模式図を示す。尚、同図によれば、アルミの膜厚増大部の巾方向領域を $1.3\mu\text{m}$ 、厚みを $0.20\mu\text{m}$ とすると、その部位での増大アルミの量は、 $1.3 \times (0.20 - 0.05) = 0.195\mu\text{m}^2$ となる。レーザー照射部領域($10\mu\text{m}$)の半分の領域($5\mu\text{m}$)にあったアルミの量は、 $5 \times 0.05 = 0.250\mu\text{m}^2$ となる。従って、それらの差を計算すると、 $0.250 - 0.195 = 0.055\mu\text{m}^2$ となる。これを長さに、換算すると、 $0.055 / 0.05 = 1.1\mu\text{m}$ となる。このことか

ら、厚みが $0.05\mu\text{m}$ のアルミ層が $1.1\mu\text{m}$ の長さだけ残留していることになり、事実上、レーザー照射部のアルミはほぼ全部、膜厚増大部に引き寄せられたと考えてよい。このように、同図による解析の結果からも、上記特徴的な現象についての説明が正しいことが分かる。

(b) 次に、単板の光ディスク（1枚のディスクにより構成される光ディスク）の場合について説明する。片面の成形ディスクの $0.05\mu\text{m}$ 厚のアルミの反射膜に同じパワーのレーザーパルスを加えた場合の実験結果を第8図（b）に示す。図に示されているようにアルミの残査が残っており、このアルミ残査が再生ノイズになるため、高い密度とエラーの少なさが要求される光ディスクの情報の2次記録用途には適していないことがわかる。又、貼り合わせと異なり第10図（b）に示すように単板ディスクの場合、無反射部がレーザートリミングされる時、必ず保護層862が破損する。破損の程度はレーザーパワーにより様々であるが、レーザーパワーを精密に制御しても破損は避けられない。さらに我々の実験では保護層862の上に数百 μm の厚さでスクリーン印刷された印刷層805が熱吸収率の大きい場合破損された。単板の場合、保護層の破損に対処するため、保護層をもう一度塗布するか保護層を塗布する前にレーザーカットすることが必要となる。いずれにしても単板方式ではレーザーカット工程がプレス工程の中に限定されるという課題が予想される。従って単板ディスクの場合、有効度は高いが、用途が限定される。

(c) 以上は、2層式の張り合わせディスクを用いて、単板のディスクと張り合わせディスクとの比較を説明した。上記説明からわかるように、1層式の張り合わせたディスクの場合でも、2層式の場合と同様の効果が得られる。従って、ここでは、第12図（a）、（b）等を用いて、1層式の場合について、更に説明

する。第12図(a)に示すように反射層802の一方は、ポリカからなる透明基板801で、もう一方は硬化した状態の接着層804と基板により充填された密閉状態となっている。この状態で、パルスレーザーを集束させ加熱すると、反射層802に本実験の場合70nsの短い時間に $5\mu\text{J}$ /パルスの熱が $10\sim 20\mu\text{m}$ の直径の円形のスポットに加わる。このため瞬時に融点である 600°C に達し熔融状態になる。熱伝導により近接した透明基板801のごく一部が溶け、接着層804も一部が溶ける。第12図(b)に示すようにこの状態で熔融したアルミは表面張力により、両側に張力が加わるため、溶けたアルミは境界部821a、821bに集まり、集中部822a、822bが形成され再び固まる。こうしてアルミの残査のない無反射部584が形成される。よって、第10図(a)に示すように貼り合わせディスクにすることにより、レーザートリミングした場合ははっきりとした無反射部584が得られる。単板の場合に発生する保護膜の破壊による外部環境への反射層の露出は、レーザーパワーを最適値より10倍以上上げてみられなかった。レーザートリミングの後、第12図(b)に示すように無反射部584は2枚の透明基板801によりサンドウィッチ構造になるとともに両側が接着層804により、外部の環境から遮断されているため環境の影響から保護されるという効果がある。

(d) さらに、ディスクを2枚張り合わせることによる、他の利点について、説明する。バーコードで二次記録した場合、第10図(b)に示すように、単板ディスクでは不正業者が、保護層を除去することによりアルミ層を露出させられる。このため、正規ディスクのバーコード部にアルミ層を再度蒸着し、再度別のバーコードをレーザートリミングすることにより、暗号化されていないデータ部を改ざんされる可能性がある。例えば、ID番号を平文、もしくは主暗号と分離して記

録した場合、単板では改ざんされ、他のパスワードでソフトの不正使用が行われる可能性がある。しかし、第10図(a)のように貼り合わせディスクに二次記録した場合、貼り合わせディスクを2枚にはがすのは困難である。このことに加えて、はがす時にアルミ反射膜が部分的に破壊される。海賊版防止マーキングが破壊された場合、海賊版ディスクと判別され、作動しなくなる。従って、貼り合わせディスクの場合不正改ざんした場合の歩留りが悪くなり、経済的に不正改ざんが抑制される。特に、2層式の貼り合わせディスクの場合、ポリカ材料は温度湿度の膨張係数をもつため、一旦はがした2枚のディスクの1層と2層の海賊版防止マーキングを数 μm の精度で貼り合わせて量産することは不可能に近い。従って、2層の場合、さらに防止効果は高くなる。こうして張り合わせディスク800にレーザートリミングすることにより鮮明な無反射部584のスリットが得られることが明らかになった。

以上の説明(a)～(d)で、光学マーキング無反射部の作成技術に関して説明した。

(C) 次に、作成されたマーキング位置の読み取り工程を説明する。

第15図は、光ディスクの製作過程における、光学マーキング無反射部を検出するための低反射光量検出部586を中心としたブロック部である。又、第16図は、低反射部のアドレス・クロック位置検出の原理図である。尚、以下の説明では、便宜上、1枚のディスクから構成された光ディスク上の無反射部を読み取り対象とした場合の動作原理について説明する。この動作原理は、2枚のディスクを張り合わせた光ディスクの場合にも勿論当てはまる。

第15図に示すように、ディスク800を低反射部位位置検出部600を有するマーキング読み取り装置に装着し、マーキングを読み取った場合、ピットの有無

による信号波型 8 2 3 と無反射部 5 8 4 の存在による信号波型 8 2 4 は信号レベルが大きく異なるため、簡単な構成の回路で、第 9 図 (a) の波形図に示すように明確に区別できる。

この波形をもつ無反射部 5 6 4 の開始位置と終了位置は、第 1 5 図のブロック図の低反射光量検出部 5 8 6 によって容易に検出される。そして、再生クロック信号を基準信号とすることにより、低反射部位置情報出力部 5 9 6 において位置情報が得られる。

第 1 5 図に示すように、低反射光量検出部 5 8 6 の比較器 5 8 7 は光基準値 5 8 8 より低い信号レベルのアナログの光再生信号を検出することにより、低反射光量部を検出する。検出期間中、第 1 6 図の (5) のような波形の低反射部検出信号を出力する。この信号の開始位置と終了位置のアドレスとクロック位置を測定する。

さて、光再生信号は、AGC 5 9 0 a をもつ波形整形回路 5 9 0 により、波形整形されデジタル信号となる。クロック再生部 3 8 a は波形整形信号より、クロック信号を再生する。復調部 5 9 1 の、EFM 復調器 5 9 2 は信号を復調し、ECC は誤り訂正し、デジタル信号が出力される。EFM 復調信号は物理アドレス出力部 5 9 3 において、CD の場合サブコードの Q ビットから MSF のアドレスがアドレス出力部 5 9 4 から出力され、クレーム同期信号等の同期信号が同期信号出力部 5 9 5 より出力される。クロック再生部 3 8 a からは復調クロックが出力される。

低反射部アドレス/クロック信号位置信号出力部 5 9 6 においては、 $n-1$ アドレス出力部 5 9 7 とアドレス信号、そしてクロックカウンタ 5 9 8 と同期クロック信号もしくは復調クロックを用いて、低反射部開始/終了位置検出部 5 9

9により低反射部584の開始点と終了点を正確に計測する。この方法を第16図の波形図を用いて具体的に説明する。第16図の(1)の光ディスクの断面図のように、マーク番号1の低反射部584が部分的に設けられている。第16図(2)のような反射信号つまり第16図(3)のようなエンベロープ信号が出力され、反射部において、光量基準値588より低くなる。これを光量レベル比較器587により検出し、第16図(5)のような低反射光量検出信号が低反射光量検出部586から出力される。又、第16図(4)の再生デジタル信号に示すように、マーク領域は反射層がないため、デジタル信号は出力されない。

次に、この低反射光量検知信号の開始、終了位置を求めるためには、アドレス情報と第16図(6)の復調クロックもしくは同期クロックを用いる。まず、第16図(7)のアドレス n の基準クロック605を測定する。 $n-1$ アドレス出力部597により、予め、アドレス n の一つ前のアドレスを検知すると、次のsync604はアドレス n のSyncであることがわかる。このsync604と低反射光量検知信号の開始点つまり基準クロック605までのクロック数をクロックカウンタ598でカウントする。このクロック数を基準遅延時間TDと定義し、基準遅延時間TD測定部608が測定し、記憶する。

読み取り用再生装置により、回路の遅延時間が異なるためこの基準遅延時間TDは読み取り用再生装置により異なる。そこで、このTDを用いて時間遅れ補正部607が時間補正を行うことにより、設計の異なる読み取り用再生装置においても低反射部の開始クロック数が正確に測定できるという効果がある。次に第16図(8)のように次のトラックの光学マークNo. 1に対する開始、終了アドレス・クロック数を求めるとアドレス $n+12$ のクロック $m+14$ が得られる。TD= $m+2$ であるから、クロック数は12に補正されるが説明では $n+14$ を

用いる。この読み取り用再生装置により、基準遅延時間TDを求めなくとも、ばらつく遅延時間の影響をなくすもう一つの方法を述べる。この方法は、第16図(8)のアドレス n のマーク1ともう一つのマーク2の相対的な位置関係が一致しているかを照合することにより、正規ディスクかどうかを判別できる。つまり、TDを変数として無視し、測定したマーク1の位置 $A1=a1+TD$ とマーク2の位置 $A2=a2+TD$ の差を求めると $A1-A2=a1-a2$ となる。同時に暗号を復号したマーク1の位置 $a1$ とマーク2の位置情報 $a2$ の差 $a1-a2$ と一致するかを照合することにより正規ディスクかどうかを照合できる。この方式であるとより簡単な構成で基準遅延時間TDのバラつきを補正した上で位置を照合できるという効果がある。

(D) つぎに暗号書き込み工程を説明する。(C)において読み取られた位置情報は、後の(2)で詳しく述べるようにして暗号化(デジタル署名化)され、バーコード等の方法で、光ディスクに書き込まれる。その様子を示すのが、第3図である。即ち、第3図(1)においてパルスレーザーにより、反射層がトリミングされ、同図(2)のようなバーコード状のトリミングパターンが形成される。再生装置側(プレーヤ側)では同図(3)のように、波形が部分的に欠落したエンベロープ波形が得られる。欠落部は通常のピットによる信号では発生しない低いレベルの信号を生じさせるので、これを第2スライスレベルのコンパレータでスライスすると同図(4)のような低反射部の検出信号が得られる。同図(5)でこの低反射部検出信号からPWM復調部621により、暗号を含む信号が復調される。

以上は、光ディスク作成側の各種工程について説明した。次に、このようにして、完成した光ディスクをプレーヤ側で再生するための、再生装置(プレーヤ)について、第41図を用いてその構成と動作を併せて説明する。

同図において、最初に光ディスク 9102 の構成を説明する。光ディスク 9102 に形成された反射膜（図示省略）には、マーキング 9103 が施されている。そのマーキング 9103 の位置が、光ディスクの製造段階において、位置検出手段によって検出され、その検出された位置がマーキングの位置情報として光ディスクに暗号化されて、バーコード 9104 で書き込まれている。

位置情報読み取り手段 9101 は、そのバーコード 9104 を読み取って、内蔵する復号化手段 9105 によって、そのバーコードの内容を復号化して出力する。マーキング読み取り手段 9106 は、マーキング 9103 の現実の位置を読み取って、出力する。比較判定手段 9107 は、位置情報読み取り手段 9101 に内蔵された復号手段 9105 による復号結果と、マーキング読み取り手段 9106 による読み取り結果とを比較し、両者が所定の許容範囲内で一致しているか否かを判定する。一致している場合は、光ディスクを再生するための再生信号 9108 を出力し、一致していなければ、再生停止信号 9109 を出力する。制御手段（図示省略）は、それらの信号に従って、光ディスクの再生動作を制御し、再生停止信号が出された場合は、不正に複製された光ディスクである旨の表示を表示部（図示省略）に行って、再生動作を停止させる。ここで、マーキング読み取り手段 9106 は、マーキング 9103 の現実の位置を読み取る際に、復号化手段 9105 の復号結果を利用してももちろんよい。

この様な再生装置によれば、不正に複製された光ディスクを検知して、その再生を停止することが出来、事実上不正な複製を防止出来る。

ここで、光ディスクの製造からプレーヤ側の再生についての説明を終えて、それらの内容に関連する、付随的事項について説明する。

(A) 低反射部の位置情報リストである低反射部アドレス表について説明する。

(a) 即ち、予め工場において、海賊版防止マーク作成工程により、無作為にレーザーマーキングを形成する。この様にして、形成されたレーザーマーキングは、同じ形状のものは作れない。次の工程では各ディスク毎に低反射部584を上述したようにしてDVDの場合、 $0.13\mu\text{m}$ の分解能で測定し、第13図(a)に示すような低反射部アドレス表609を作成する。ここで、第13図(a)は、本実施例により作成される正規のCDの低反射部アドレス表などを表した図であり、第13図(b)は、CDが不正複製されたものである場合の図である。この低反射部アドレス表609を第18図に示すような一方向関数で暗号化し、第2図に示すように、ディスクを最内周部に、バーコード状の反射層のない低反射部群584c~584eを、2回目の反射層形成工程において、記録する。もしくは第14図に示すように、CD-ROMの磁気記録部67に記録してもよい。第18図は、暗号化に用いる一方向関数によるディスク照合のフローチャートであり、第14図は、ディスク作成装置、及び専用の記録再生装置のブロック図である。第13図に示すように正規のCDと不法に複製されたCDでは低反射部アドレス表609、609xが大幅に異なる。その要因の1つは、上述したように、レーザーマーキングは、同じ形状のものが作れないからである。更に、ディスクにおいて予め割り当てられたセクタのアドレスが、ディスクの原盤相互間で相違することも両者が大幅に異なる第2の要因である。

即ち、ここで、第13図を参照しながら、マーキングに関して、正規ディスクと海賊版ディスクとで得られる位置情報の違いを説明する。同図では、上記第1、第2の要因が重なっている場合である。又、マーキングは、ディスク上に2つ形成されている。即ち、マーク番号1のマーキングに対して、正規のCDの場合、アドレス表609に示されているように第1マークは、論理アドレスA1のセク

タの中の開始点より262番目のクロックの位置にある。1クロックはDVDの場合、 $0.13\mu\text{m}$ であるため、この精度で測定されている。次に、海賊版CDの場合、アドレス表609xに示されているように、アドレスA2のセクタの中の81番目のクロックの位置にある。このように、第1マークの位置が正規ディスクと海賊版ディスクでは違うことから海賊版ディスクを発見することができる。同様に、第2マークの位置も異なる。この正規ディスクと位置情報を一致させるには、アドレスA1のセクタの262番目の位置の反射膜を1クロック単位つまり、 $0.13\mu\text{m}$ の精度で加工しないと海賊版ディスクは作動しない。

従って第14図のように、再生装置においてこの暗号化された表を復号して、正規の表をつくり、照合プログラム535により照合することにより、正規のディスクと不法複製されたディスクを区別することができ、複製ディスクの動作を停止できる。第16図の例では第17図に示すように正規のディスクと不正複製されたディスクでは低反射部アドレス表609、609xの値が異なる。第16図(8)のように正規ディスクではマーク1の次のトラックでは開始終了は $m+14$ 、 $m+267$ であるが、第16図(9)のように不法複製されたディスクでは $m+21$ 、 $m+277$ となり異なる。こうして第17図に示すように低反射部アドレス表609、609xの値が異なり複製ディスクを判別できる。この低反射部アドレス表609をもつディスクを不法複製業者が複製する場合は、彼らは第16図(8)に示すように再生クロック信号の分解能で正確にレーザートリミングを行う必要がある。DVDディスクの場合、第27図(5)に示すように再生クロックパルスの周期Tをディスク上の距離に換算した場合 $0.13\mu\text{m}$ になる。従って、不法複製するには $0.1\mu\text{m}$ のサブミクロンの分解能で反射膜を除去することが要求される。確かに光ディスク用の光ヘッドを用いた場合、サブミクロンの精度でCD

-Rのような記録膜に記録できる。しかし、この再生波形は第9図(c)のようになり、第9図(a)のような特異な波形824は反射膜を除去しない限り得られない。

(b) 従ってこの反射膜をとり除く海賊版の量産方法としてはYAG等の大出力レーザーを用いたレーザートリミングが1番目の方法として考えられる。現状では最も精度の高い工作用レーザートリミングの加工精度は数 μm しか得られない。半導体のマスク修正用レーザートリミングにおいても1 μm が加工精度の限界であるといわれている。つまり、レーザートリミングでは0.1 μm の加工精度を量産レベルで達成することは難しい。

(c) 二番目の方法として、現在サブミクロンの加工精度を達成しているのは、超LSIの半導体マスクの加工用のX線露光装置やイオンビーム加工装置が知られているが、非常に高額な装置で1枚あたりの加工時間も要するため、ディスク1枚毎に加工すると1枚のコストは高額なものとなる。従って、現行では殆どの正規ディスクの販売価格を上回るコストとなり、採算がとれなくなり、海賊版ディスクを作る意味がなくなってしまう。

(d) 以上のように第1の方法であるレーザートリミングでは、サブミクロン加工が困難なため、海賊版ディスクの量産が困難である。又、第2の方法であるX線露光等のサブミクロン加工技術では、1枚あたりのコストがかかりすぎて、経済面で海賊版ディスクの生産が無意味となる。従って、低コストのサブミクロンの量産加工技術が実用化されるまでの間、海賊版の複製は防止される。このような技術が実用化されるのは遠い将来のことであるので海賊版の生産は防止される。また2層ディスクの各層に低反射部を設けた場合、第33図に示すように上下のピットを合わせて精度よく貼りあわせないと海賊版ディスクは複製できないため、防止効果はさらに上がる。

(B) 次に、低反射部のディスク上の配置角度を所定のように特定する事項について説明する。

本発明では、反射層レベルつまり低反射部マーキングだけで十分な海賊版防止効果がある。この場合、原盤は複製品であっても防止効果がある。しかし、原盤レベルの海賊版防止技術と組み合わせることにより、さらに防止効果を高められる。低反射部のディスク上の配置角度を第13図(a)の表532aと表609のように特定すると、海賊版業者は原盤の各ピットの配置角度の状態まで正確に複製する必要がある。海賊版のコストが上がるため、抑制効果がさらに上がる。

(C) 次に、ここで本発明のポイントをまとめる。本発明では正規業者は数十 μm の加工精度の汎用のレーザトリミング装置で加工すれば、正規のディスクが作れる。測定精度には0.13 μm が要求されるが、これは民生用のDVDプレーヤーの一般的な回路で測定できる。この測定結果を暗号の秘密鍵で暗号化することにより正規ディスクが生産できる。つまり、正規業者は秘密鍵と0.13 μm の測定精度の測定器のみが要求され、要求される加工精度は2~3桁悪い数十 μm である。従って、一般のレーザ加工装置でよい。一方、海賊版業者は、秘密鍵をもっていないため、正規ディスクの暗号をそのままコピーせざるを得ない。この暗号の位置情報つまり、正規ディスクの位置情報に対応した物理マークを0.13 μm の加工精度で加工する必要がある。つまり正規業者の加工機より2桁高い加工精度の加工機で低反射部マークを作成する必要がある。この2桁高い加工精度つまり、0.1 μm の精度による量産は技術的にも経済的にも近い将来を考えると困難である。このため、海賊版ディスクはDVD規格存続中は防止されることになる。つまり、本発明の一つのポイントは一般的に測定精度が加工精度より数桁高いことを利用している点にある。

以上のことはCLVの場合、前述のように原盤のアドレスの座標配置が異なることを利用している。第19図に実際のCDのアドレスの位置について測定した結果を示す。一般に、ディスク原盤は、一定回転数つまり等角速度(CAV)でモーターを回転させて記録されたものと、一定の線速度つまり等線速度(CLV)でディスクを回転させて記録されたものの2種類がある。CAVディスクの場合、論理アドレスは所定の角度上に配置されるため、論理アドレスと原盤上の物理的配置角度は何度原盤を作成しても全く同じである。しかし、CLVディスクの場合、線速度しか制御しないため、論理アドレスの原盤上の配置角度はランダムになる。第19図の実際のCDの論理アドレスの配置測定結果に示すように、全く同じデータを原盤作成装置で記録しても、トラッキングピッチや開始点や線速度が毎回微妙に違い、この誤差が累積されるため、物理的配置が異なる。第19図では、第1回目に作成した原盤の各論理アドレスのディスク上の配置を白丸で示し、第2回目、第3回目に作成して原盤の配置を黒丸、三角で示す。このように原盤を作成する毎に論理アドレスの物理配置がことなることがわかる。尚、第17図は、正規のディスクと不正複製されたディスクの低反射部アドレス表の比較図である。

以上、原盤レベルの防止方式を述べた。これは、同じ論理データから原盤作成装置を用いてCDやDVDのようなCLV記録の原盤を作成した場合、第19図に示すように、正規ディスクと海賊版ディスクでは、各ピットの原盤上の物理的配置が原盤毎に異なる。この点に着目して正規ディスクと海賊版ディスクの識別を行うものである。原盤レベルの海賊版防止技術は単純に正規ディスクのデータのみを複製した論理レベルの海賊版を防止できる。しかし、最近ではより高度の技術をもつ海賊版業者が登場し、正規ディスクのポリカ基板を溶かすことにより、

正規ディスクと全く同じ物理形状のレプリカの原盤を作成することが可能となっている。この場合、原盤レベルの海賊版防止方式は破られてしまう。この新たな海賊版ディスクの生産を防止するため、本発明では反射膜にマーキングする反射層レベルの海賊版防止方式を考案した。

さらに、本発明の方法では、上述のように、例え原盤が同じでも、原盤を用いて成形されたディスク一枚毎に反射膜作成工程で反射膜を一部削除することによりマーキングを作成する。従って、ディスク毎に低反射部マーキングの位置や形状が異なる。サブミクロンの精度で正確に反射膜を部分的に削除することは、通常工程では不可能に近い。従って本発明のディスクを複製することは経済的に成立しないため、複製防止の効果は高い。

尚、第20図に低反射部アドレス表による複製CDの検出フローチャート図を示す。再生装置の光ヘッドや回路等の設計により、光マークの検出に要する遅延時間が、ごくわずかであるが異なる。この回路遅延時間TDは設計時点もしくは量産時点で、予測できる。光マークはフレーム同期信号からのクロック数つまり時間を測定して位置情報を得る。このためこの回路遅延時間の影響により、光マークの位置情報の検出データに誤差が生じる。すると正規のディスクまで海賊版ディスクであると判定してしまい正規の使用者に迷惑を与える。そこで、回路遅延時間TDの影響を軽減する工夫を述べる。又、ディスクの購入後についた傷により、再生クロック信号が途切れるため光マークの位置情報の測定値に数クロックの誤差が生じることから、これについての対策として、ディスクに第27図の許容誤差866と合格回数867を記録し、再生時における測定値の許容誤差を実状に応じて認めるとともに、合格回数867に達した時点で、再生を許可することによりディスクの表面の傷による誤差の許容範囲をディスクの出荷時に著作

極者がコントロールできる工夫を第20図を用いて説明する。

即ち、第20図において、ステップ865aでディスクを再生して、本発明のバーコード記録部もしくはピット記録部より暗号化された位置情報を入手する。ステップ865bで復号もしくは署名検証を行い、ステップ865cで光マークの位置情報リストを得る。次に再生回路の遅延時間TDが再生装置の第15図の回路遅延時間記憶部608aの中に入っている場合はステップ865hより、TDを読み出し、ステップ865xへ進む。TDが再生装置にない時、もしくはディスクに測定命令が記録されている時は、ステップ865dに進み基準遅延時間の測定ルーチンに入る。アドレスNs-1を検知すると次のアドレスNsの開始位置がわかる。フレーム同期信号と再生クロックをカウントし、ステップ865fで基準の光マークを検知する。ステップ865gで回路遅延時間TDを測定し、記憶する。なお、この動作は第16図(7)を用いて後述する動作と同じである。ステップ865xでアドレスNmの中にある光マークを測定する。ステップ865i, 865j, 865k, 865mにおいてはステップ865d, 865y, 865f, 865yと同様にして、光マークの位置情報をクロック単位の分解能で検出する。次にステップ865nで、海賊版ディスクの検知ルーチンに入る。まず、回路遅延時間TDを補正する。ステップ865pで、第27図に示すディスクに記録されている許容誤差866つまりtAと合格回数867を読み出し、ステップ865gで測定した位置情報が許容誤差tAの範囲に収まっているかを照合する。ステップ865rでこの結果がOKなら、ステップ865sで、照合したマーク数が合格回数に達したかをチェックし、OKならステップ865uで正規ディスクと判別し、再生を許可する。まだ、合格回数に達していない場合はステップ865zへ戻る。ステップ865rでNOの場合は、ステップ865fで誤

検出回数がNAより少ないかをチェックしOKの場合のみ、ステップ865sへ戻る。OKでない時は、ステップ865vで不正ディスクと判定して停止する。

以上のようにして、再生装置の回路遅延時間TDをICのROM内に記録してあるので、より正確に光マークの位置情報が得られる。又、ディスクのソフト毎に許容誤差866と合格回数を設定することにより購入後のディスクについての傷に対して、実態に合わせて海賊版ディスクの判定基準を変更できるので、正規ディスクを誤判別する確率が低くなるという効果がある。

(D) ここで、2枚のディスクを張り合わせた光ディスクにおける光学マーキング無反射部の読み取りに関する説明における、上記動作原理では、触れなかった点を中心として述べる。

即ち、第16図のように開始位置のアドレス番号、フレーム番号、クロック番号が1T単位の分解能つまり、DVD規格においては一般プレーヤーで0.13 μ mの分解能で本発明の光学マークを正確に測定できる。第16図の光学マークのアドレスの読みとり方法をDVD規格に適用したものを第27図と第28図に示す。第16図と同じ動作原理であるため第27図、第28図の信号(1)(2)(3)(4)(5)の説明は省略する。

ここで、CDの場合の低反射部の位置検出原理図である第16図と、DVDの場合の第27図、第28図との対応について述べる。

第16図(5)は、第27図(1)、第28図(1)に対応する。第16図(6)の再生クロック信号は、第27図(5)、第28図(5)に対応する。第16図(7)のアドレス603は、第27図(2)、第28図(2)に対応する。

第16図(7)のフレームSync604は、第27図(4)、第28図(4)に対応する。第16図(8)の開始クロック番号605aは、第27図(6)の再生チャンネル

クロック番号に対応する。第16図(7)の終了クロック番号606に代えて、第27図(7)、第28図(7)では6bitのマーキング長を用いてデータの圧縮を計っている。

図示するようにCDとDVDでは基本的に検出動作は同じであるが、第1の違いとして第27図(7)の1bitのマークの層識別子に603aに示すように、低反射部が1層であるか、2層であるかの識別子が入っている点が異なる。DVDの2層の場合、上述のように防止効果が高まる。第2の違いとして線記録密度が倍近く高いため、再生クロックの1Tが $0.13\mu\text{m}$ と短くなり、より位置情報の検出分解能が上がり、防止効果が高い。

第27図の場合、2層の反射層をもつ2層式の光ディスクを用いた場合の一層目の信号を示し、信号(1)は1層目の光学マークの開始位置を検出した状態を示す。第28図は2層目の信号の状態を示す。

2層目を読み出す時は、第15図の1層2層部切換部827より焦点制御部828に切り換え信号を送り1層から2層へ焦点駆動部829により焦点を切り換える。第27図からアドレス(n)であることがわかり、信号(4)のフレーム同期信号をカウンタでカウントすることにより、フレーム4にあることがわかる。信号(5)のPLL再生クロック番号がわかり、信号(6)の光学マーキング位置データが得られる。この位置データを用いて、一般の民生用DVDプレーヤで光学マークを $0.13\mu\text{m}$ の分解能で測定することができる。

(E) 次に、2枚のディスクを張り合わせた光ディスクのさらに関連事項を説明する。

第28図は、2層目にできた光マーキングのアドレス位置情報を示す。第7図の工程(b)で示したように、レーザー光は1層、2層を貫通させて同じ穴で開

けるため、第1層の反射層802にできた無反射部815と第2反射層825にできた無反射部826とは同じ形状をしている。この状態を第33図に表わした斜視図で示す。本発明では透明基板801と第2基板803を張り合わせた後にレーザを貫通させて2層に同じマークを作成する。この場合、1層と2層はピットの座標配置が異なることと、貼り合わせ時の1層、2層間の位置関係はランダムであるため、1層と2層では各々異なるビット部にマークが形成され、全く異なる位置情報が得られる。この2つの位置情報を暗号化して海賊版防止ディスクを作成する。このディスクを不正に複製しようとした場合、各々2層の光学マークを $0.13\mu\text{m}$ 程度の精度で一致させる必要がある。前述のように $0.13\mu\text{m}$ つまり $0.1\mu\text{m}$ の精度で光マークで光マークとピットを一致させて複製することは現状では無理であるが、将来、低コストで $0.1\mu\text{m}$ の加工精度で1層ディスクを大量にトリミングできる量産技術が実現する可能性はある。この場合でも2層貼り合わせディスク800の場合、上下2枚のディスクが同時トリミングされるので、上下2枚のピット配置および光学マークを数 μm の精度で合わせる必要がある。しかし、ポリカ基板の温度係数等によりこの精度で張り合わせることは、不可能に近い。このため2層のディスク800にレーザを貫通させ光学マークを作成した場合、複製が著しく困難な海賊版防止マークが得られる。このため海賊版防止効果が高くなるという効果が得られる。以上のようにして、海賊版防止処理が施された光ディスクが完成する。この場合、海賊版防止用途の場合、単板のようにディスク工程とレーザカット工程が分離できない場合、レーザカット工程と一体となった暗号化工程及び暗号の秘密鍵の処理はディスク工場の中で行うことになる。つまり、単板方式はソフト会社のもつ暗号用の秘密鍵をディスク工場に渡す必要があり、暗号の機密性が大幅に低下する。これに対し、本

発明の1つの対応である貼り合わせディスクにレーザー加工する方式はレーザートリミングがディスク製造工程とは完全に分離できる。従って、ソフトメーカーの工場でもレーザートリミングと暗号化作業が行なえる。ディスク工場にソフトメーカーがもつ暗号の秘密鍵を渡す必要がなく、暗号の秘密鍵がソフトメーカーの外部に出ないため、暗号の機密性が大幅に向上する。

(2) 次に、上述したように、(1)において簡単に述べられた、(A) マーキング位置情報等の暗号化(デジタル署名)等、光ディスクの位置情報等復号再生等について詳細に説明する。又、(B) その他の、海賊版防止に関する様々な工夫についても述べる。

(A) 暗号化(デジタル署名)とその再生について説明する。

(a) 単純な暗号化(デジタル署名)の場合:

(RSA関数を用いた場合の説明)

まず、暗号化を行う際に利用する関数として、RSA関数のようなメッセージリカバリー型署名方式の関数を用いて暗号化する場合の例を、第22図、第24図に示すフローチャートを参照しながら説明する。

第22図に示すように、大きなルーチンとしては、光ディスクメーカー側における、マーキングの位置情報を測定するステップ735aと、位置情報を暗号化(又は、署名)するステップ695と、再生装置側における、位置情報の復号化(又は、署名を検証あるいは認証)するステップ698と、正規の光ディスクかどうかの照合を行うステップ735wとから構成されている。

まず、ステップ735aでは、ステップ735bで、光ディスク上のマーキングの位置情報を測定する。その位置情報をステップ735dで圧縮し、ステップ735eで圧縮した位置情報Hを得る。

ステップ695では、圧縮された位置情報Hの暗号を作成する。まず、ステップ695で、512bitもしくは1024bitのdと、256bitもしくは512bitのpとqの秘密鍵を設定し、ステップ695bで、RSA関数による暗号化を行う。位置情報Hを、図中に示したMであるとする、Mをd乗しmod nの演算を行い暗号Cを得る。ステップ695dで暗号Cを光ディスク上に記録する。これにより、光ディスクが完成し、光ディスクの出荷が行われる(ステップ735k)。

再生装置では、ステップ735mで光ディスクが装着され、ステップ698で暗号Cを復号する。具体的には、ステップ698eで暗号Cを再生し、ステップ698fで公開鍵としてのe,nを設定し、ステップ698bで暗号Cを復号するために、暗号Cをe乗し、更にその値のmod nを演算し平文Mを得る。この平文Mというのは、圧縮された位置情報Hである。尚、ステップ698gでエラーチェックを行ってもよい。エラーがない場合は位置情報が改ざんされていないと判断し、第24図のディスクの照合ルーチン735wへ進む。エラーがある場合は正規のデータでないと判断して停止する。

さて、次のステップ736aでは圧縮された位置情報Hを伸張し、元の位置情報が復元される。ステップ736cではの位置情報に示されている光ディスク上の位置に、実際にマーキングがあるかをどうかを測定する。ステップ736dでは、復号により得られた位置情報と、実際に測定した位置情報の差が許容範囲内かを照合する。ステップ736eでは、照合がOKならステップ736hへ進み、光ディスク内のソフトやデータの出力もしくはプログラムを動作させる。もし照合結果が許容範囲内でない場合、即ち双方の位置情報が一致しない場合は、不正に複製された光ディスクであると表示し、ステップ736gで停止させる。RS

Aの場合は、暗号だけを記録すればよいので、小さい容量でよいという効果がある。

(楕円関数を用いた場合の説明)

次に、暗号化を行う際に利用する関数として、別の方式であるインプリント型の署名方式の楕円関数を用いた場合の、第23図、第24図に示すフローチャートを参照しながら説明する。

第23図等 to 示すように、大きなルーチンとしては、光ディスクメーカ側における、マーキングの位置情報を測定するステップ735aと、その位置情報の認証暗号(すなわち署名)を演算するステップ735fと、再生装置側における、位置情報の認証(すなわち署名検証)を行うステップ735nと、正規の光ディスクであるかの照合を行うステップ735wとから構成されている。

まず、ステップ735aから、ステップ735eまでは、RSA関数の場合と同様である。

ステップ735fでは、圧縮された位置情報Hの認証暗号を作成する。まず、ステップ735gで、秘密鍵として、 X (128 bit 以上) と、 K とを設定し、ステップ735hで、楕円曲線上の点で公開のシステムパラメータ G を決め、 $f(x)$ を一方向性関数 (one direction function) とした場合、 $R = f(K \times G)$ を求めた後、 $R' = f(R)$ を求め、 $S = (K \times R' - H) X^{-1} \bmod Q$ の式により、認証暗号としての R 、 S を生成する。ステップ735jで認証暗号 R 、 S と、圧縮された位置情報の平文 H とを光ディスク上に記録し、ステップ735kでディスクを出荷する。

再生装置では、ステップ735mで光ディスクが装着され、ステップ735nで、位置情報の認証演算をおこなう。

まず、ステップ735pで装着された光ディスクから、認証暗号 R と S と、圧

縮された位置情報Hとを再生する。ステップ735rで、公開鍵Y、G、Qを設定し、ステップ735sで認証演算を行い、 $A = SR^{-1} \bmod Q$ 、 $B = HR^{-1} \bmod Q$ から $f(A \times Y + B \times G)$ を求め、ステップ735tで、この値がRと一致するかをチェックする。一致した場合は位置情報が改ざんされていないと判断し第24図の光ディスクの照合ルーチン735wへ進む。一致していない場合は正規のデータでないと判断して停止する。

さて、次のステップ736aから、ステップ736gは、RSA関数の場合と同様である。即ち、不正に複製された光ディスクであると判定した場合、その旨を表示し、ステップ736gで停止させる。尚、楕円関数の場合は、RSA関数の場合と比べて、演算時間が短くて済むので、再生開始までの時間が短く出来るという効果があり、民生用の再生装置への応用に適している。

(b) マスタ鍵とサブ鍵等を用いて、複雑に暗号化（デジタル署名）する場合：

すなわち、マーキングの位置情報だけでなく、光ディスクに入力されるソフト内容の特徴情報や、海賊版防止識別子をも暗号化（デジタル署名）の対象とし、さらに、マスタ鍵とサブ鍵の2つの暗号鍵をもつ点にある。尚、ここでの具体例としては、秘密鍵系暗号関数と公開鍵系暗号関数を併用した例を示す。

ここで、具体例の詳しい説明に入る前に、基本的な部分を理解するために、先ず第40図を用いて、本例の基本的な構成を説明する。

尚、この基本的説明では、公開鍵系暗号関数により暗号化処理を行う場合の例であり、秘密鍵系暗号関数による暗号化処理は登場しない。そのため、公開鍵系暗号用のマスタ秘密鍵、公開鍵系暗号用のサブ秘密鍵は、それぞれ単にマスタ秘密鍵、サブ秘密鍵と呼ぶ。又、公開鍵系暗号用のマスタ公開鍵、公開鍵系暗号用

のサブ公開鍵は、それぞれ単にマスタ公開鍵、サブ公開鍵と呼ぶ。

第40図に示すように、鍵管理センター9001は、マスター秘密鍵をその秘密性が保たれる様に厳重に管理しており、後述するソフトメーカ9002と通信回線9003で結ばれている。そして、ソフトメーカ9002から暗号化の依頼があった場合、ネットワーク9003を介して送られた暗号化の対象を、そのマスター秘密鍵を用いて、暗号化する部門である。

ソフトメーカ9002は、ここでは説明を単純にするために、ディスク工場も含むものとする。従って、ソフトメーカ9002は、ソフトの作成作業に加えて、第1図で述べたディスク工場での作業も行う部門である。即ち、映画のソフトを入力した光ディスクを製造する際に、海賊版業者の複製を防止するための暗号化の処理を併せて行う。この暗号化処理を実施するために、ソフトメーカ9002は、鍵管理センター9001から、専用のサブ秘密鍵を渡されている。以上が、光ディスクのメーカ側の構成である。

一方、上記光ディスクを利用するユーザ側として、プレーヤ9004がある。プレーヤ9004は、光ディスクを再生するための装置であり、内蔵されたROMには、鍵管理センターが管理しているマスタ秘密鍵に対応したマスタ公開鍵があらかじめ格納されている。そして、不正に複製された光ディスクの再生を停止する機能を有している。

以上の様な構成において、次に動作説明を行う。

(b-1) 先ず、ソフトメーカ9002が行う暗号化に関する工程を中心に述べる。

最初に行われる暗号化処理(第1暗号化処理)は、ディスクの金型を作る段階における暗号化であり、その暗号化された情報が、ディスクの金型の形状に反映

される。そして、最後に行われる暗号化処理（第2暗号化処理）は、レーザートリミングを行ってマーキングを作成した後の段階での暗号化である。

（1-1）第1暗号化処理では、第2暗号化処理の際に用いるサブ秘密鍵に対応するサブ公開鍵と、ソフト特徴情報と、海賊版防止識別子とを用いて暗号化し、その情報を通信回線9003により鍵管理センタ9001へ転送する。ここで、ソフト特徴情報とは、例えば、光ディスクに書き込む映画ソフトの内容を表した情報であり、各映画ソフトによって全て異なる固有の特徴情報である。又、海賊版防止識別子とは、製造された光ディスクが、海賊版防止の処理が施されたものであるか否かを検知出来るようにするためのものである。第2暗号を利用した海賊版防止の処理が施された光ディスクの識別子は”1”であり、その処理が施されていない場合は、”0”となる。本例では、この識別子は、当然、”1”となる。

（1-2）鍵管理センタ9001は、ソフトメーカ9002から転送されてきた上記情報を、自らが管理するマスタ秘密鍵を用いて暗号化して、それを再びソフトメーカ9002へ返送する。このよにして生成された暗号を第1暗号と呼ぶ。

（1-3）ソフトメーカ9002は、返送されてきた第1暗号を映画ソフト等と共に、ディスクの金型（又は、原盤）へ記録する。

（1-4）ソフトメーカ9002は、このよにして製造した金型を使って、ディスクを成型する。

（1-5）次に、ソフトメーカ9002は、成型したディスクを用いて光ディスクを作成して、上述した様にレーザートリミングを行い、光ディスク上にマーキングを形成する。

（1-6）更に、ソフトメーカ9002は、そのマーキングの位置を検出して、

その検出の結果得られた位置情報を、自らが持っているサブ秘密鍵を用いて暗号化する。このようにして暗号化されたものを第2暗号と呼ぶ。この第2暗号は、位置情報を暗号化しているため、同じ金型から成型されたものであっても、1枚毎の光ディスクによって、全て異なるものであり、第1暗号と相違する点である。

(1-7) 最後に、ソフトメーカ9002は、この第2暗号を光ディスクにバーコードとして記録する。これにより光ディスクが完成する。

(b-2) 次に、この様にして完成された光ディスクを、ユーザが購入し、プレーヤ9004を用いて再生する際の動作について説明する。

(2-1) 先ず、プレーヤ9004は、光ディスクに記録された第1暗号を読み出し、ROMに格納されているマスタ公開鍵を使って、第1暗号即ち、サブ秘密鍵に対応するサブ公開鍵と、ソフト特徴情報と、海賊版防止識別子とを合成して暗号化されたものを復号する。

(2-2) 一方、プレーヤ9004は、光ディスクに、現実に記録された映画ソフトの内容から、そのソフト特徴情報を抽出する。この抽出したソフト特徴情報と、(2-1)で、復号により得られたソフト特徴情報とを照合し、一致しなければ、不正に複製された光ディスクであるとの判断により、それ以降の再生動作を停止する。一致すれば、更に次に進む。

(2-3) 即ち、(2-1)で、復号により得られた海賊版防止識別子が、“1”であるか、“0”であるかを調べる。“0”であれば、次に説明する処理を行わず、直ちに再生動作に入る。しかし、“1”であれば、更に、次に進む。

尚、これにより、第2暗号を利用した海賊版防止処理が、施されていない光ディスクであっても、正規に識別子が“0”に設定されている限り、プレーヤ9004は、再生を行うものである。又、海賊業者が、この識別子が“0”となるよ

うにして、不正な複製を行おうとしても無理である。この識別子は、上述した様にソフト特徴情報などと共に合成されたのち、マスタ秘密鍵で暗号化されているからである。

(2-4) ここでは、先ず、光ディスクに記録されている第2暗号を読み出す。そして、その第2暗号即ち、位置情報を暗号化したものを、(2-1)で、復号により得られたサブ公開鍵を用いて復号する。

(2-5) 復号された位置情報を用いて、その位置情報に対応する光ディスク上の位置に、実際にマーキングが存在するか否かを調べる。その結果、実際に測定されたマーキングの位置情報と、(2-4)で復号された位置情報とを照合する。不一致であれば、不正に複製された光ディスクであると判断して、再生動作を停止し、一致していれば、正規な光ディスクであると判断して、それ以降の再生を行う。

以上で、アウトラインの説明を終わり、次に、更に具体的な説明を行う。

即ち、第32図に示すようにソフトコンテンツから各映像ソフトの各チャプターの時間構成を示すTOC情報や画像圧縮パラメータやタイトル名等の各々ソフトに固有なソフトパラメータをチェックサム演算とガロア体等の演算やSHAやMD5のような一方向性ハッシュ関数864aにより128bitから256bitに圧縮したソフト特徴情報863を、ソフト特徴抽出手段864により抽出圧縮し、更にそれに加えて、各ソフトメーカー専門のサブ公開鍵861と、著作権識別子としての海賊版防止識別子865とを1つのデータに合成し、ステップ866a、866bで公開鍵系暗号のマスタ秘密鍵を用い、暗号化した上で、ステップ866eで原盤867に本体のソフトとともに記録する。

尚、秘密鍵系と、公開鍵系とを併用する方式を採用した場合は、ステップ86

6 c では秘密鍵系暗号用マスタ秘密鍵を用い、ステップ 8 6 6 d で暗号化し、ステップ 8 6 6 e で原盤 8 6 7 に記憶する。

こうして原盤工程は完了する。原盤に記録した海賊版防止識別子 8 6 5 は、そのソフトが海賊版防止付かどうかを示すフラグが 1 b i t、低反射部バーコード付かどうかを示すフラグが 1 b i t スランブル付かどうかを示すスランブル識別子 9 6 5 a のフラグが 1 b i t、ソフトのダビングを防止するかを示すフラグが 1 b i t 等の著作権保護フラグが 4 b i t 以上入っているもので、そのソフトが本来どのような著作権保護すべきかどうかを規定している。海賊版防止識別子 8 6 5 とサブ公開鍵 8 6 1 は、ソフト固有のソフト特徴情報 8 6 3 と合成されて公開鍵系暗号のマスタ秘密鍵により暗号化されているため改ざんできない。

海賊版防止識別子 8 6 5 とサブ公開鍵 8 6 1 は各ソフトに固有なソフト特徴情報 8 6 3 とともに 1 つのデータとして一括して秘密鍵により暗号化されている。

このソフト特徴情報 8 6 3 は 2 5 6 b i t とした場合、2 の 2 5 6 乗の組み合わせがある。このため、ある特定の映画ソフトをオーサリングしたデータのソフト特徴情報を抽出した場合、他のソフトのソフト特徴情報と一致する確率は 2 の 2 5 6 乗分の 1 となり、まず一致することはない。MD 5 や SHA の一方向性ハッシュ関数を用いた場合はハッシュ値、つまりソフト特徴情報 9 6 3 が 2 5 6 b i t の場合、現在得られる大型計算機を 1 0 の 1 8 乗年の間、演算しつづけないとハッシュ値が同じ 2 つのソフトコンテンツをみつけ出すことができないとされており、ソフトの入れ替えは困難となる。オーサリングした特定のソフトに対してソフト特徴情報は 1 つの値だけ存在し、かつ他のソフトと同じ値になることはない。

さて、特定のソフト特徴情報と海賊版防止識別子 8 6 5 とサブ公開鍵 8 6 1 は

一括して暗号処理されているため、この2つのどの値も変更することはできない。こうしてオーサリング後の特定のソフトに対する海賊版防止識別子865およびサブ公開鍵861は特定されることになる。

ここで、海賊版防止識別子865を原盤に記録する点について詳しく述べる。

各ソフトに対して、海賊版防止識別子865をどのように付与するかはソフトの著作権者の選択の問題である。光ディスクのソフトに海賊版防止対策を施すと、コストや手間がかかる。従って、全ての光ディスクに海賊版防止は施されず、海賊版防止もしくは本発明のバーコードのついた光ディスクとついていない光ディスクが混雑することになる。このように、海賊版防止やバーコードが付与されない正規ディスクも存在を認めると、当然再生装置はこれらのディスクを正常に再生する機能をもつ必要がある。この場合、ある海賊版対策なしディスクを再生する場合、そのソフトに対してソフト会社が正規に海賊版防止をはずした場合と、ソフト会社が海賊版防止機能付と定義したディスクのソフトを海賊版業者が海賊版防止識別子を不正に変更したものである場合の、2つのケースが考えられる。

従って、海賊版防止識別子が不正であるかを判別する手段が重要となる。

本発明では海賊版防止識別子を含む海賊版防止識別子865をソフト特徴情報とまとめて秘密鍵で暗号化し、原盤の暗号記録部に記録している。再生装置では所定の公開鍵で復号するので、いずれかを不正に変更することは防止される。

海賊版業者にできることは、ソフト特徴情報863と海賊版防止識別子865を含む第1暗号全部をそっくり入れ替えることだけである。

尚、このソフト特徴情報863を、後述する、現実に光ディスクに書き込まれた映画ソフトの中から抽出されるソフト特徴情報と区別するために、前者を第1のソフト特徴情報と呼び、後者を第2ソフト特徴情報と呼ぶこともある。両者は、

同じ映画ソフトの内容を対象としている点で同じであるが、前者は、光ディスク製造時に暗号化されて書き込まれ、後者は、再生時に現実に記録されている映画ソフトの内容を調べて、抽出される点で異なる。

第1ソフト特徴情報863はオーサリングの完了した各ソフトに固有の値であるため、別のソフトが同じ値になる確率は前述のように2の256乗分の1で殆どないといってよい。第1ソフト特徴情報863を入れ換えた場合、再生装置において第38図のステップ876a、876c、876e、876fに示す照合ルーチンによりステップ876eで現実にディスクから抽出した第2ソフト特徴情報885と一致しなくなるため、入れ替えたディスクの再生は防止される。こうして、各ソフトの海賊版防止識別子865および後述するサブ公開鍵の不正変更は防止される。このため、海賊版業者がディスクからソフトをコピーして海賊版を作成する場合、海賊版防止識別子やバーコードのないディスクを作成しようとするのが考えられる。この時、海賊版防止識別子865の海賊版防止識別子をオン("1")からオフ("0")へ設定変更する必要がある。しかし、この設定変更には第36図のステップ866aに示したマスタ秘密鍵により暗号化した第1暗号を鍵管理センタから発行してもらう必要があるが、海賊版業者に鍵管理センタが発行することは通常防止されるため、海賊版防止識別子865が不正変更されることは防止される。

つまり、第1ソフト特徴情報863と海賊版防止識別子865を一括して暗号化した第1暗号886を原盤へ記録することにより、海賊版業者は海賊版防止マークや機能のない海賊版無対策のディスクのフォーマットで、海賊版防止機能が付与されているソフトを不法に作成することが防止されるという効果がある。本発明の一つの対応であるこの手法により、海賊版対策のしていないディスクと、対

策してあるディスクとを混在させながらディスク規格を作り、世代交代しても第2世代の再生装置では全てのディスクに対して海賊版防止を実現するという大きな効果がある。尚、上記具体例では、著作権保護フラグ（識別子）として、ソフトコンテンツが海賊版防止の対象ソフトであるか否かを示す海賊版防止識別子865等を用いた例を説明した。これとは別に、ソフトコンテンツがコピー防止の対象ソフトであるか否かを示すコピー防止識別子を用いることにより、本来、コピー防止であるソフトのディスクが、コピー防止識別子を解除されて、ディスクの形態で販売されることを防止できる。

ここで、公開鍵系秘密鍵において、上記マスタ秘密鍵とサブ秘密鍵の必要性及びさらにそれら秘密鍵の具体的な構成、作用について詳述する。

本発明の海賊版防止においては二次記録できるため暗号用秘密鍵をディスク工場に渡す必要はない。しかし、全世界で生産される全てのディスク1枚毎に、暗号化センターに暗号エンコードしてもらい、暗号をネットワークで受けとる方式は通信のトラフィック量が多くなるため現実的でない。かといって、各ソフトメーカーやディスク工場に秘密鍵を渡すことはセキュリティの面で、できないという問題点がある。この問題点を解消する方法が求められている。

本発明ではこれを解消する方法としてマスタ鍵、サブ鍵方式を提供する。本発明では、鍵管理センタ（鍵発行センタ）がマスタ秘密鍵をもち外部に公開しない。一方、ソフト会社はサブ秘密鍵をもつことにより、自分のソフトのセキュリティを自分の責任で確保する。第32図を用いて、上述したように、ソフト特徴情報と各ソフト会社があつサブ公開鍵を一括してマスタ秘密鍵で暗号化し、それを第1暗号とする。再生装置では第1暗号をマスタ公開鍵で復号し、その復号されたものからサブ公開鍵が抽出される。そのため、マーキングの位置情報を暗号化し

たものとしての第2暗号を復号するのに必要となるサブ公開鍵は、不正な変更ができない。

従って、特定のソフトは特定の秘密鍵つまり、各ソフトメーカーがもつサブ公開鍵の秘密鍵でしか暗号化されないこととなる。各ソフトメーカーはこのサブ秘密鍵を用いて自由にソフトの鍵の開閉を設定できる。

逆に海賊版業者は、ソフト毎に異なるサブ秘密鍵の情報をそのソフトメーカーから盗まない限り海賊版が製造できないことになる。

ソフトメーカーは、第32図において、ディスク物理位置情報868とディスクID869を合成して、サブ秘密鍵876（第32図に合わせるために、符号を修正しました。以下同様）でステップ866fで暗号化して公開鍵系暗号859を作成し、光ディスク800にバーコード記録する。この場合、マスタ秘密鍵866aをソフトメーカーに渡さないでソフトメーカーがサブ秘密鍵876で海賊版防止ディスクを製造することができる。このため、マスタ秘密鍵のセキュリティが確保できるという効果がある。もしサブ秘密鍵が盗まれて海賊版ディスクが生産されても、その被害はサブ秘密鍵を発行したソフトのみに限定される。ソフトメーカーは新しいサブ秘密鍵とサブ公開鍵を発行すれば、それ以降のソフトの海賊版ディスクの生産は防止される。第36図、第37図の全体のシステム図に、データの流れを示す。

第36図は第32図と同じ動作であるので詳しい説明は省略する。第36図においてソフト会社871aではまず各社独自のサブ秘密鍵876を設定し、演算することによりサブ公開鍵861が求められる。このサブ公開鍵861を、記録対象のソフトのソフト特徴情報863と合成し鍵発行センター872にインターネット等のネットワークで送信する。鍵発行センター872ではマスタ秘密鍵8

66aで合成信号を暗号化しマスタ公開鍵暗号858をソフト会社へ返信し、ソフト会社では、ソフトと合成し合成信号をディスク工場873へ送り原盤867に記録し、ディスク800が製造される。第37図へ進み、ソフト会社871bではディスク800にマーキングを行い、マークの位置情報を読みとり、位置情報をサブ公開鍵に対応したサブ秘密鍵876により、暗号化しディスク800bにパルスレーザー813でバーコード記録する。詳しい記録の動作は説明済みのため省略する。

次に、このようにして、作成された光ディスクを再生する場合の、再生装置における海賊版防止の動作を第38図を用いて、さらに詳しく具体的に説明する。

まずこの動作は大きく、ソフト照合ステップ874とディスク照合ステップ875に分けられる。ソフト照合ステップ874のステップ876aでは、まず、ディスク800より第1暗号を再生し、ステップ876cで再生装置のROMに入っているマスタ公開鍵を用いて、ステップ876bで、第1暗号を平文化する。ステップ876dで第1ソフト特徴情報863とサブ公開鍵861の平文を入手し、ステップ876eで、一方向性ハッシュ関数を用いて抽出した第2ソフト特徴情報とを、ステップ876fで照合する。ステップ876gで照合が正しくない時は動作を停止し、正しい時は、ステップ876hでサブ公開鍵を出力させる。海賊版業者がサブ公開鍵やソフト属性を変更した場合、照合が一致せず、不正再生は阻止される。こうして正規のサブ公開鍵が再生装置において得られる。

ディスク照合ステップ875のステップ876kではサブ公開鍵を入力し、ステップ876mでは第2暗号つまり公開鍵系暗号859（第32図参照）を再生し、ステップ876nではサブ公開鍵を用いて平文化し、ステップ876pでマークの位置情報を得る。この場合、マークの位置情報はサブ公開鍵のサブ秘密鍵

876 (第32図参照) が漏れない限り改ざんされない。ステップ876dでレーザによりディスクに形成されたマーキングの現実の位置を読み取り、ステップ876rで照合する。ステップ876sでNoならステップ876tで停止し、“海賊版ディスクです。”という表示を出す。Yesならステップ876uで再生を続ける。

以上のような再生装置の構成により、不正に複製したディスクについては、ソフトメーカー保有のサブ秘密鍵876が盗まれない限り、また無反射部のマークを超サブミクロン例えば $0.13\mu\text{m}$ の精度でレーザトリミングさせかつ2枚のディスクをミクロンオーダーで正確に貼り合わせない限り、再生装置において再生動作が行われない。従って、事実上、海賊版を作ることはできない。これにより海賊版が防止されるという効果がある。

(c) 公開鍵系と秘密鍵系の暗号関数を併用する例のより詳しい説明：

本実施例の暗号化における第1の特徴としては、1枚毎の光ディスクにおけるマーキングの位置情報等を暗号化する際に、公開鍵系暗号関数と秘密鍵系暗号関数の2つの関数を用いている点である。

ここでは本発明による公開鍵系暗号を用いた海賊版防止方式を現実に実用化する場合の課題と実現方法を述べる。尚、公開鍵系暗号とは、上述した位置情報を公開鍵系暗号関数(例えば、RSA関数)を用いて、暗号化したものをいう。

機密性保持の面からは、全ての再生装置に公開鍵系暗号復合器を設けて本発明の海賊版防止の公開鍵系暗号を復号するのが望ましい。しかし、512bitの公開鍵暗号をCPUで処理する時間は、32bit 50MHzのCPUを用いて0.3秒を要する。一方、現在の民生機器のDVDプレーヤ制御用ICは8bitの1chipマイコンが主流である。このCPUでは公開鍵を処理するのに数

分以上かかる。これは数分待たないとDVDの画像が出てこないことになり、製品には導入できないといった課題がある。

このように現時点では、公開鍵系暗号は、民生用製品のCPUでは処理できないため、当分の間、民生用の再生機器は処理量の少ない秘密鍵系暗号用復号器を搭載せざるを得ない。秘密鍵系暗号は、暗号デコーダの情報から暗号化秘密鍵を容易に逆解読することができるため、その時点で秘密鍵系暗号は海賊版防止効果がなくなる。従って将来、逆解読が困難な公開鍵系暗号に移行させることが不可避といえる。

秘密鍵系暗号と公開鍵系暗号には、全く互換性がない。このため、将来、単純に秘密鍵系暗号を公開鍵系暗号に切り換えると、秘密鍵系暗号デコーダをもつ第1世代のプレーヤで、公開鍵系暗号をもつ第2世代の光ディスクを復号・再生できなくなる。また第1世代の秘密鍵系暗号をもつ光ディスクを将来のプレーヤで再生することもできなくなる。もし、この再生を可能に設定すると、海賊版業者は秘密鍵系暗号の秘密鍵を逆解読し、これを用いて秘密鍵暗号を作成し、海賊版ディスクを作成するので、海賊版ディスクが大量に販売されることになる。秘密鍵系で暗号化されたディスクを将来のプレーヤでも再生可能とした場合、公開鍵系暗号を使っても海賊版は防止できない。

このことから、将来、秘密鍵系から公開鍵系へ再生装置の暗号デコーダが移行しても、新しい公開鍵系暗号デコーダをもつ再生装置で初期の光ディスクを正常に再生し、かつ海賊版ディスクの不法再生を防止する互換性維持の工夫が必要となる。

この互換性の要求を満たす本発明の方法を開示する。第39図に示すように本発明の光ディスクでは秘密鍵系暗号記録部879と公開鍵系暗号記録部880の

双方をもつ。製造方法は第29図を用いて後述する。まず第39図のこの光ディスクを再生する時、第1世代の秘密鍵系暗号デコーダ881をもつ再生装置では、正規ディスクの秘密鍵系暗号記録部879から秘密鍵系暗号デコーダ881によりディスク固有の第1物理特徴情報（位置情報が暗号化されたものに対応）を平文化する。又、ディスクの第2物理特徴情報（測定された位置情報に対応）を測定し、双方の物理情報を照合する。

正規ディスクの場合は、ステップ878aに示すように双方の物理特徴情報が一致するので通常に再生される。

海賊版ディスクの場合は、ステップ878cに示すように照合結果が一致しないので、不正再生は防止される。秘密鍵系暗号が破られるまでは防止されるが、上述のように将来、秘密鍵系暗号が破られた後は海賊版業者は秘密鍵系暗号を不正生成することにより不正ディスクを大量に作成する。

従って、ステップ878dに示すように第1世代の再生装置の秘密鍵系デコーダ881では秘密鍵系暗号しかチェックしないので照合結果が一致し、海賊版ディスクが不正に再生される。しかし、将来のこの時点においては第2世代の公開鍵系暗号デコーダ882をもつ再生装置が大勢を占めているため、第1世代の再生装置における海賊版ディスクの不正再生の影響は小さい。

この第2世代の再生装置では、本発明の正規ディスクは公開鍵系暗号をもつためステップ878bに示すように正常に再生される。一方、海賊版ディスクを再生した場合、秘密鍵系暗号の逆解読のいかんにもかかわらず、ステップ878eに示すように再生装置は公開鍵系暗号のみをチェックするため、ステップ878eに示すように、公開鍵系暗号の海賊版防止機能が働き、第2世代の再生装置では海賊版がほぼ完璧に防止される。

本発明の場合、全てのディスクに秘密鍵暗号 8 7 9 に加えて公開鍵暗号 8 8 0 を第 1 世代の再生装置の出荷段階から予め搭載してある。従って、まず第 1 段階では第 1 世代の再生装置の 8 b i t マイコンで暗号の処理ができるため、秘密鍵系暗号レベルの海賊版防止ができる。次に第 2 段階つまり将来、秘密鍵系暗号が破られた時点においては、主流となっている第 2 世代の公開鍵系暗号デコーダにより完全な海賊版防止ができる。このため、世代交代が起こっても初代のメディアとの互換性を完全に保ちながら第 2 世代の再生装置により中断することなく、海賊版防止がほぼ完璧に実現するという世代交代時の互換性を確保する効果がある。

なお、上記説明では低反射部マーキング方式、つまり反射層レベルの海賊版防止方式に適用した場合の例を説明したが、第 1 3 図のような原盤の物理特徴情報を用いる原盤レベルの海賊版防止方式に適用しても同様の世代交代時の互換性を確保する効果が得られる。

以上説明した例では、暗号化を行なう場合、同一の暗号化対象を、公開鍵系暗号関数と秘密鍵系暗号関数を個別に利用して、それぞれ暗号化し、この双方をディスク上に記録することを特徴としている。

従って、現行の 8 ビットマイコンによる秘密鍵系暗号関数により暗号化された暗号を復号する復号器を持ったプレーヤーから、将来の 3 2 ビットマイコンによる公開鍵系暗号関数により暗号化された暗号を復号する復号器を持ったプレーヤーに移行しても、本例による光ディスクであれば、何れのタイプのプレーヤーに対しても、有効に使用できるという効果がある。

(B) その他の工夫について説明する。

(a) 次に、別の具体例として、公開鍵系と秘密鍵系の併用タイプであり、そ

の暗号化対象となるものが、ソフト特徴情報、ID番号、マーキングの位置情報の場合について説明する（第29図参照）。ここで、ID番号とは、ディスク毎に与えられた、各ディスクを識別するための番号である。後述するディスクID（ディスクID番号とも呼ぶ）も、このID番号と同じ意味である。本例と上記具体例（第32図、第36図、第37図参照）との主なる相違点は、（1）上記具体例では、ソフト特徴情報は、ディスクの原盤に第1暗号として書き込まれ、一方、マーキングの位置情報は、成型されたディスクに第2暗号として書き込まれるのに対して、本例では、ソフト特徴情報、ID番号、マーキングの位置情報の全てが合成されて暗号化され、既に成型されたディスクに書き込まれるという点である。又、（2）上記具体例では、マスタ秘密鍵とサブ秘密鍵を利用して、2段階の暗号化を行うのに対して、本例では、サブ秘密鍵に対応する鍵は使用せず、言うならばマスタ秘密鍵による暗号化を行う点である。

即ち、第29図に示す様に、秘密鍵系秘密鍵834により、上述の合成された信号を秘密鍵系暗号化部832においてエンコードする。又、公開鍵系秘密鍵833により、上述の合成された信号を公開鍵系暗号化部831においてエンコードする。このように、公開鍵系と秘密鍵系の暗号を併用する。これにより、現在の再生装置はマイコンの処理速度が遅いため、秘密鍵系暗号しか復号できない問題点が、解決できる。将来の再生装置は32ビット等の処理速度が速いマイコンを用いてセキュリティが強い公開鍵系のみを復号し、海賊版チェックを行うので、海賊版は、ほぼ完全に防止できる。秘密鍵系が将来被られても、その時点においては公開鍵系プレーヤが大勢を占めているので、海賊版は実質的に防止できる。秘密鍵系と公開鍵系暗号を同時に媒体に記録しておくことによりプレーヤの世代交代が起こっても旧世代のプレーヤで再生できるとともに実質的に海賊版が防止

できるという効果がある。

(b) 次に、同図を用いて、更にバーコードの変調記録方式について詳細に述べる。

第29図において、バーコード記録装置(PWM記録装置)845は、ディスクに暗号化された情報を書き込むためのものである。

まず、反射層802、又は第2反射層825に設けられた無反射部815の位置情報を光マーク位置検出手段600で検出する。この検出方法は第15図等を用いて説明したので省略する。光マーク位置情報と、ID発生部546によるID番号と、ソフト特徴情報とを合成手段830により合成する。ソフト特徴情報はソフトコンテンツの一部をSHA等の一方方向ハッシュ関数で特徴抽出し128ビットや160ビットのハッシュ値を求めることにより得る。ID番号発生部546は、第14図を用いて説明したので省略する。この物理特徴情報の合成信号を暗号化部830において公開鍵系秘密鍵833を用いてRSA等の公開鍵系暗号化部831においてエンコードする。

上記の公開鍵系の暗号と、秘密鍵系の暗号を合成部835で合成し、記録回路836のエラー訂正符号化部837の中で、リードソロモン符号化部838とインターリーブ部839によるインターリーブ/リードソロモンのエラー訂正を行う。この場合のインターリーブ長はディスク上のバーストエラーとしてCD並みつまり、2.38mm以上の長さの傷によるバーストエラーに対して、エラー訂正できるように設定することにより、民生用途の最悪条件で発生するディスク上の傷に対して、本発明のバーコード記録データのエラーが訂正されるという効果がある。

更に、同図を用いて、パルス巾変調方式の原理を述べる。また、この方式はマ

スタ秘密鍵による第1暗号とサブ秘密鍵による第2暗号を使わなくてもよい。この方式では、ソフト特徴情報と位置情報とID番号を合成して暗号化している。年間数十億枚ROMディスクは生産されている。このためディスクのマークが偶然非常に複製しやすい位置パターンのディスクが製造される可能性がある。この複製しやすい位置情報のマークとこの位置情報の正規の暗号の組み合わせで、海賊版が製造されてしまう。第29図においては、位置情報がソフト特徴情報とともに暗号化もしくは署名されている。従って、この位置情報は、このソフト特徴情報と切り離せない。つまり、複製容易なマークが製造できても、それに対応するソフトコンテンツの海賊版ディスクしか製造できず、被害が、大巾に限定されるという効果がある。なお、この暗号は原盤に記録しても良い。

エラー訂正符号化された信号はパルス間隔変調部840により、PWM信号に変調される。レーザーにより直線を描く場合、線巾を正確に制御してバーコードを作成することは難しい。従って、第30図に示すように、本発明ではパルス間隔を1T, 2T, 3T, 4Tの4値に更け分けマーク843b, 843c, 843d, 843eを各々例えば00, 01, 10, 11と符号化することにより、2bitのデータを1本のバーコードで伝送することができる。第30図の線巾と記録速度の関係表842に示すように、線巾=10 μ mの時、ROMディスク800のリードインエリアにPIMバーコードを記録した場合、1周で5.6Kbitの情報がディスクの完成品に追記記録できることがわかる。

第31図の信号(1)は無反射部の検出信号を示す。

まず、信号群は、間隔Tの3本のパルス857a, 857b, 857cからなる開始位置を示す同期信号領域858がある。次に基準時間Tを測定する基準時間Tを測定する基準時間領域で4Tのブランクがある。線幅10 μ mの場合T=

20 μm である。そして2次記録データが入っている第1記録領域860が約1 Kbitである。そして100 μm 以上のブランク861aを空けて、3回目の記録、3次記録データの第2記録領域862aが記録される。具体的には、販売店で、スクランブル解除用のパスワード等が記録される。

(c) このHMS T方式で二次、三次記録できるバーコードの利用方法について述べる。

第35図に示すようにソフトメーカーでは、工程(2)ではディスク1枚ごとに異なるID番号やユーザーとの秘密通信用のプライベートキーを記録したディスク844bを作成しても良い。このディスク844c、844dは何もしなくとも再生できる。

又、後述する第21図において示したように、磁気記録再生回路のMFMM変復調部磁気ヘッドをPWM(PIM)変復調部レーザーに置き換えることにより、本発明のHMS T方式の記録再生回路が得られる。

(d) ここで、第35図において、ディスク作成の別の具体例を示す。即ち、別の応用として、第35図に示す工程(3)では、スクランブルしたMPEG映像信号等の情報をディスク844eに記録する。ここで、MPEGスクランブルの動作説明を簡単に行う。MPEGの画像圧縮信号はAC成分の可変長符号部と固定長符号部に分けられ、各々に乱数加算部があり、スクランブル化される。本発明では、スクランブル解除信号を一方向関数の暗号エンコーダーで暗号化する。また、画像圧縮制御部の圧縮プログラムの一部を暗号エンコーダーにより圧縮している。このため、複製業者が暗号エンコーダーを不正なものに入れ替えることが困難となる。従って、正規のディスクのみがサブ公開鍵で復号される。

次に、再び、第35図に戻り、上述した工程(3)で作成されたディスク84

4 e に対しての、次の工程 (4) 以降での処理の内容を説明する。

即ち、第 35 図において、ソフト会社では同図に示す工程 (4) においてディスク ID 番号とスクランブル解除情報を復号するためのサブ公開鍵をマスタ秘密鍵で暗号化した暗号をバーコードで二次記録したディスク 844 f を作成する。このディスク 844 f は、スクランブルされているので、このディスク単独では再生はできない。ここで、ディスク ID 番号は、上述した ID 番号と同じ意味である。工程 (5) では、販売店が客からディスクの代金を受け取った後にサブ公開鍵に対応しているサブ秘密鍵でディスク ID 番号を用いてパスワードを作成し、ディスクに三次記録する。このあとは、ディスク 844 g にはパスワードが記録されているため、再生装置でディスクスクランブルされ再生可能となる。コンピュータプログラムの場合はインストール可能となる。この方式を用いると、代金の支払われていないディスクが万引きされても映像のスクランブルや暗号化が解除されないため画像やソフトが再生されない。このため、万引きが無意味になり、防止されるという効果がある。

(e) ここで、一旦、第 35 図を利用した説明を終えて、第 21 図を参照しながら同図に示す記録回路のついた再生装置として、光再生装置に磁気記録再生回路を組み合わせた記録再生回路における磁気記録再生回路を中心に構成及び動作を説明する。尚、第 21 図では、光再生装置と合体した磁気記録再生回路を用いて説明しているが、通常の光再生装置とフロッピイドライブの組み合わせでもよい。

同図では磁気再生回路の中の復調器として MFM 復調器 30 d とは別の方式の第 2 復調器 6 b 2 をもち、切換部 661 で切り換えられる。これは対応する変調器は工場しかもたないため、再生はできるが完全な記録はできない。従って、工場で特殊変調された領域を記録した場合、特殊変調信号は記録されない。ドライ

ブ側ではCPU 665により、この領域で特殊変調信号を再生しない限り、記録できないように制御している。従って、論理的な、Write Once領域といえ、1回だけ記録できる。従って再生装置のROM 699に記録されたドライブID 699a等のマシンIDを、光ディスクの磁気記録部もしくはフロッピーディスクのWrite Once領域に記録すると、ユーザーのドライブでは改ざんすることができなくなり、許可された台数以上の不正インストールを防止することができる。ここで、ドライブIDとは、再生装置毎に与えられた、各再生装置を識別するための番号である。また、このマシンIDはパソコンのIDでもよい。ネットワークのインターフェース部14により、ネットワーク664に、接続された第2パソコン663の中のHDD等をみて、同じドライブIDやマシンID番号のプログラムが起動や動作をしないように監視させる。こうして、不正コピーされたソフトの動作を防止する。

また、本発明のレーザでマーキングする記録方式を用いると磁気方式のようにディーラーでディーラーコードを記録したり等の二次記録ができるが、本発明の特徴的な部分ではないので、詳しい説明はここでは省略する。

レンタルビデオ店では恒久的にパスワードを記録すると、万引きされた場合、使用されてしまう。この場合は工程(6)に示すように、レンタル店でスクランブルされているディスク844jを客に渡す。ステップ851gでスクランブル解除のためのパスワードは、ディスクIDもしくは後述するドライブIDをサブ秘密鍵を用いて算出する。ステップ851jでプリンタでレシートに印刷して、客に手渡す。ステップ851uに示すように電話等で客に通知しても良い。

客は自宅の再生装置においてステップ851rのスクランブル解除処理を行う。まずステップ851sで暗号よりスクランブル識別子とソフト特徴情報とサブ公

開鍵で復号化する。復号されたソフト特徴情報と実際にソフトコンテンツから一方向ハッシュ関数で抽出したソフト特徴情報を照合し、一致しているか検証する。検証できない時は、不正とみなし、ストップする。ステップ851xでスクランブル識別子がOFFの場合は、ステップ851pで再生を許可する。スクランブル識別子がONの場合はステップ851kでユーザがパスワードをテンキーで入力し、パスワードはサブ公開鍵で演算する。ステップ851tでさらにディスクIDもしくは/かつドライブIDを用いた演算を行ないパスワード演算結果がディスクIDもしくはドライブIDにする場合のみ、ステップ851pで、スクランブルもしくは暗号化を解除し、再生もしくは動作を所定の日数だけ許可する。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみたくなった時は、鍵発行センターへ電話し電話で、そのソフトのパスワードをステップ851uで通知してもらい、ステップ851kで入力することにより、ディスクの他のソフトを再生することができる。

第35図の工程(5)(6)のセルビデオ販売店、レンタルビデオ店における動作を第34図を用いてより具体的に説明する。セルビデオ販売店ではソフトメーカーからスクランブルもしくは暗号化がかかったディスク844fを受けとり、ユーザーからの入金を確認するとバーコード記録再生装置845よりディスク844fのディスクID番号、サブ公開鍵のデータをPOS端末846経由でパスワード発行センター852に送信する。小規模な店舗システムの場合パスワード発行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはPOS端末の中にあっても良い。パスワード発行センターはステップ851qでディスクID番号と時間情報を入力し、ステップ851sで演算を行い、ステップ851tで、サブ秘密鍵を用いて暗号化し、ステップ851gでパスワードを発行しネットワ

ーク 8 4 8 と POS 端末 8 4 6 を介してバーコード記録装置 8 4 5 にパスワードを送り、記録されたディスク 8 4 4 g が客に渡される。このディスク 8 4 4 g は、そのまま再生できる。

次にレンタル店における動作を詳しく述べる。まずスクランブルの解除されていない ROM ディスク 8 4 4 f を店頭に陳列する。客が特定の ROM ディスク 8 4 4 f を指定した場合、うずまき型にスキャンする回転型の光学ヘッド 8 5 3 を内蔵した円形バーコードリーダ 8 5 0 を手にもち、透明ケース入りのディスク 8 0 0 の中心におしつけることにより、ディスク 8 4 4 f の無反射部 8 1 5 による反射層のバーコードを読み取り、ディスク ID 番号を読み取る。商品コードは無反射部 8 1 5 の本発明のバーコードから読みとつてもよいし、原盤のピット記録領域外の内周部に予め記録されプレスされた既存の記録方式による円形バーコードから読みとつても良い。これらの情報は POS 端末 8 4 6 により処理され、レンタル料金が決済されるとともに、前述のようにディスク ID 番号に対応したパスワードがステップ 8 5 1 g において発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ 8 5 1 r で用いたように日付情報を加えて、ディスク ID 番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しないため、レンタルの場合例えば 3 日間の貸し出し期間をパスワードの中に設定できるという効果がある。

さて、こうして発行されたスクランブル解除のためのパスワードはステップ 8 5 1 i において、貸出日、返却日、レンタルのタイトル料金とともにレシート 8 4 9 に印刷され客にディスクとともに渡される。客はディスク 8 4 4 j とレシート 8 4 9 を持ち帰り、ステップ 8 5 1 k でパスワードを第 2 5 図の情報処理装置 6 7 6 のテンキー等の入力部 8 5 4 に入力することによりパスワードはディスク

ID番号と演算されてマスタ暗号デコーダ534に入力され、公開鍵を用いて平文化される。この平文が所定の条件を満たすか平文データ照合部715で照合され、正しいパスワードである場合のみサブ暗号デコーダ718でプログラムのデータをデスクランブルし、映像出力させる。

この場合、パスワードに時間情報が含まれている場合、時計部855の日付データと照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するID番号とともにメモリ755の不揮発メモリ755aにストアされ、ユーザーは一度パスワードを入力すると2度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

これまでの実施例では、主にディスクにディスクID番号を付与したディスクID方式を用いて、説明した。しかしディスクにディスクIDがついていない場合は、ドライブのドライブIDを利用する必要がある。ここでは、ドライブIDを単独で用いた場合およびドライブIDとディスクIDの双方を用いた場合のスクランブル解除のパスワードの作成と照合の動作について具体的に説明する。

第35図においてソフトのスクランブル解除用にドライブIDに関連するパスワードを用いる場合は、まず、再生装置のROM内のドライブID699aを電話もしくはパソコン通信により、第34図の信号部851zからパスワード発行センターへ送信する。パスワード発行センターでは、ステップ851qでこのドライブIDとソフトのIDを用いて、ステップ851sで演算しステップ851tでサブ秘密鍵により暗号化し、ステップ851gでパスワードを作成する。ステップ851uで、パスワードを、電話もしくは、パソコン通信を用いてユーザーのパソコンを含む再生装置の通信部85zへ送信する。ユーザーはステップ8

51kにおいてパスワードを入力し、ステップ851mでサブ公開鍵で復号演算する。ステップ851tで、ドライブIDと演算結果を照合し、一致しない時は停止し、一致する時はステップ851pで再生もしくは動作を実行する。

ここでドライブIDの方式とディスクID方式の得失について述べる。ディスクIDを用いた場合は、パスワードはそのディスク1枚にのみ有効である。従って、全てのドライブで動作するため、映画ソフト等に適している。しかし、パソコンのビジネスソフトの場合は、どんなドライブでもインストールできると、1枚のディスクから複数のパソコンに不正インストールされてしまう。

ドライブID方式が、1台のドライブでしか動作しない点が映画ソフトでは欠点になる。しかしパソコンソフトの場合は利点となる。1回しかインストールする必要のないビジネスソフトの場合、ドライブID方式のパスワードプロテクト解除方式により正規の1台のドライブ以外のドライブを用いてパソコンに不正インストールできないという効果がある。

しかし、ドライブIDはマシンのEPROMにIDを書き込むだけであり、容易に改ざんされる。このため、同じドライブIDのドライブが販売されると、大量に不正インストールされるおそれがある。一方、本発明のディスクIDの改ざんが困難であることを述べた。第34図のステップ851qにおいてディスクIDとドライブIDとドライブの双方のパスワードを作成し、ステップ851tで両方のIDをチェックするように変更することにより、ディスクIDの方は改ざんされない。このため、同じドライブIDのドライブが大量に出回っても、ディスクIDが1枚しか存在しないことにより、大量の不正インストールが抑制されるという効果がある。

また上述のように、ドライブID方式とディスクID方式は各々利点と欠点を

もち、用途により利点異なる。1回インストールするだけのコンピュータソフト用には主にドライブID、何回も再生する映画、音楽ソフトにはディスクIDが使われると思われる。従って、再生装置は両方に対応する必要がある。図42のフローチャートを用いてドライブIDとディスクIDの双方に対応する動作を説明する。インストールが開始されると、まず、ステップ901aでスクランブル識別子がONかどうかをチェックする。識別子がOFFの場合にソフトがスクランブルされている場合は不正であるので停止する。ONの場合にソフトがスクランブルされていない時も停止する。既に述べたように、このスクランブル識別子は改ざんできないため不正を防ぐことができる。ステップ901cでパソコンをネットワークによりパスワード発行センターに接続する。ステップ901dでユーザーIDを入力し、ステップ901eで再生装置のドライブIDがある時はドライブIDをパスワード発行センターへ送信する。パスワード発行センターでは入金を確認した後、ドライブIDとソフトIDから暗号のサブ秘密鍵を用いて、暗号化と演算を行いパスワード生成し、ユーザーのパソコンではパスワードをサブ公開鍵で演算、複号し、パソコンのマシンIDもしくは、ドライブのドライブIDと照合する。照合が一致しない場合は停止し、照合が一致した場合はステップ901nでインストールプログラムを動作させる。この場合、具体的にはステップ901kでパスワードをドライブID番号と演算する時、プログラムの暗号解除キーを出力して暗号もしくはスクランブルを解除してもよい。

さてステップ901eに戻り、ドライブIDがない時はステップ901hでディスクにディスクIDが記録されているかチェックし、ディスクIDがない場合は停止する。ディスクIDがある時は、ステップ901cでディスクIDとソフトIDをパスワード発行センターへ送信する。パスワード発行センターではク

レジット会社と交信しクレジットによるオンライン入金決済確認後ステップ 901j でディスク ID とソフト ID により、サブ秘密鍵を用いてパスワードを作成する。ユーザーのパソコンではステップ 901m でこのパスワードをサブ公開鍵で復号し、照合 OK ならプログラムインストールもしくはソフトの再生を実行する。

このように、ドライブ ID、ディスク ID のどちらにも対応できるので、様々な ID をもつソフトに対応して不正インストールを防止しながら正規インストールできるという効果がある。

このようにして、ディスクの物理 ID を一方向性の暗号エンコーダにより暗号化することにより複製防止の安全度を高めることができる。

以上のように、本実施例によれば、2 枚のディスクを張り合わせた光ディスクの反射層上に無反射部を作成し、少なくともその位置情報を暗号化して、同じ光ディスク上に書き込むことにより、従来に比べてより一層複製が困難となる。これにより、不正な複製を行う、いわゆる海賊版の作成を事実上不可能にすることができる。

以上述べたところから明らかなように本発明は、複製防止能力を従来に比べてより一層向上させることが出来るという長所を有する。

なお、本実施例によれば、暗号化の工夫において、第 32 図等を用いて説明した様に、フォーマットの原盤物理特徴情報 876 を公開鍵データやソフト特徴情報と合成して暗号化することにより原盤にも海賊版防止チェックをかけられるのでよりセキュリティが高くなる。

又、第 26 図ではオンラインショッピング会社のネットワークセキュリティを向上させる方法を開示したが、秘密通信用のプライベートキーをオンラインショ

ッピング会社が全ディスクに予め二次記録しユーザーに配布することによりプライベートキーを封書でユーザーに送る必要がなくなり、ユーザも長い桁数のプライベートキーをキー入力する手間が省ける。また、ユーザ入力でなくなるため、プライベートキーとして、100桁以上の長い数値を用いることができるためネットワークセキュリティが大巾に向上する。

又、本発明のマーキングの位置情報は、上記実施例では、同じディスク上に書き込む場合について説明したが、これに限らず例えば、他の媒体としての他のフロッピーディスクに書き込むようにしてもよい。

又、上記実施例では、デジタル署名の技術又はデジタル署名的な技術又は暗号化技術に、楕円関数やRSA関数を応用した場合について説明したが、それに限らず、例えば、DESの秘密鍵系暗号関数等、その他の暗号化に関するいかなる技術を利用してもよいことは言うまでもない。

又、上記実施例では、位置情報を暗号化又はデジタル署名していたが、そのようなことはせずに、位置情報そのものをディスクに書き込んでもよい。その様な場合でも、マーキングとその位置情報をコピーして海賊版を作ることに對しては有効である。

又、本発明の、レーザにより消滅しない材料からなる2つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザによりマーキングが施されていることを特徴とする光ディスクは、上記実施例では、海賊版防止技術に利用した場合について説明したが、これに限らずその他の技術に応用してももちろんよい。又、本発明のこの光ディスクは、上記実施例では、接着層を間に設けて2枚の基板を張り合わせたディスクについて説明したが、これに限らず接着層は無くてもよいし、あるいは、保護層の様な他の部材

が存在してもよく、要するに、レーザにより消滅しない材料からなる2つの部材により反射膜が直接又は間接的に挟まれた構造であればよい。更に又、本発明のこの光ディスクは、上記実施例では、張り合わせるものとして、基板を用いた場合について説明したが、これに限らず例えば保護層等他の部材であってもよく、要するにレーザにより消滅しない材料からなる部材であればよい。

又、上記実施例では、世代の異なる複数の暗号の組み合わせ例として、秘密鍵系の暗号と公開鍵系の暗号の2つの暗号を組み合わせた場合を代表例として説明した。しかしながらこれに限らず、世代の異なる別の組み合わせとして、例えば、256ビットの秘密鍵を持つ公開鍵系暗号のように安全性は低い、遅いCPUで処理出来る暗号と、1024ビットの秘密鍵を持つ公開鍵系暗号のように安全性は高い、高速のCPUでないと処理出来ない暗号との組み合わせのように、安全性のレベルの異なる公開鍵系暗号の組み合わせでも、同様の世代交代時の互換性保持効果が得られる。また、秘密鍵系と低安全度の公開鍵系暗号と高安全度の公開鍵系暗号の3つの世代の異なる暗号の組み合わせでもよい。

産業上の利用可能性

以上説明したように、本発明は、例えば、データの書き込まれたディスクの反射膜にレーザによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはデジタル署名された形で、前記ディスクに書き込まれている光ディスクであり、これによって、複製防止能力を従来に比べてより一層向上させることが出来た。

請 求 の 範 囲

1. ディスクに形成された反射膜にマーキングを施すマーキング生成手段と、
前記マーキングの位置を検出するマーキング位置検出手段と、
前記検出された位置をマーキングの位置情報として出力する位置情報出力手段
と、
を備えたことを特徴するマーキング生成装置。
2. 少なくとも前記出力された位置情報又はその位置情報に関する情報を前記
ディスクに、又は別の媒体に書き込むための位置情報書き込み手段を備えたこと
を特徴する請求項1記載のマーキング生成装置。
3. 前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はそ
の位置情報に関する情報を暗号化する暗号化手段を有し、その暗号化された内容
を前記ディスクに書き込むことを特徴する請求項2記載のマーキング生成装置。
4. 前記暗号化手段は、前記暗号化する場合に、公開鍵系暗号関数の秘密鍵又
は、秘密鍵系暗号関数の秘密鍵を用いることを特徴する請求項3記載のマーキン
グ生成装置。
5. 前記暗号化手段は、
ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と
公開鍵系暗号関数のサブ公開鍵とを、前記公開鍵系暗号関数のマスタ秘
密鍵により暗号化する第1暗号化手段と、
前記位置情報又はその位置情報に関する情報を前記サブ公開鍵に対応
するサブ秘密鍵により暗号化する第2暗号化手段とを有し、
前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き
込むとは、

前記第 1 暗号手段により暗号化された内容と、前記第 2 暗号化手段により暗号化された内容とを前記ディスクに書き込むことであることを特徴とする請求項 3 記載のマーキング生成装置。

6. 前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報についてデジタル署名を行うデジタル署名手段を有し、

前記少なくとも出力された位置情報又はその位置情報に関する情報を書き込むとは、前記デジタル署名を行った結果に関する情報を前記ディスクに書き込むことであることを特徴する請求項 2 記載のマーキング生成装置。

7. 前記デジタル署名手段は、前記デジタル署名する場合に、公開鍵系暗号関数の秘密鍵を用いることを特徴する請求項 6 記載のマーキング生成装置。

8. 前記デジタル署名手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とについて、前記公開鍵系暗号関数のマスタ秘密鍵によりデジタル署名する第 1 デジタル署名手段と、

前記位置情報又はその位置情報に関する情報について、前記サブ公開鍵に対応するサブ秘密鍵によりデジタル署名する第 2 デジタル署名手段とを有し、

前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き込むとは、

前記第 1 デジタル署名手段によるデジタル署名を行った結果に関する情報と、前記第 2 デジタル署名手段によるデジタル署名を行った結果に関する情報とを前記ディスクに書き込むことであることを特徴する請求項 6 記載のマーキ

ング生成装置。

9. 前記位置情報書き込み手段は、同一の対象である位置情報に関して、複数種類の暗号化あるいはデジタル署名技術を用いて処理した情報を並存させるように、書き込みすることを特徴とする請求項2記載のマーキング生成装置。

10. 前記公開鍵系暗号関数は、RSA関数又は楕円関数であることを特徴する請求項4、5、7、又は8に記載のマーキング生成装置。

11. 前記ディスクは、2枚のディスクを張り合わせるることにより作成されていることを特徴する請求項1～10の何れか一つに記載のマーキング生成装置。

12. ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜が形成されたディスクを少なくとも1つ含む2枚のディスクを張り合わせるステップと、

その張り合わされたディスクの前記反射層に対して、レーザーによりマーキングの形成を行なうステップと、

を備えたことを特徴する光ディスクのレーザーマーキング形成方法。

13. ディスクに形成された反射膜にマーキングを施し、前記マーキングの位置を検出し、少なくとも前記検出された位置がマーキングの位置情報として出力された、そのマーキングの位置情報又はその位置情報に関する情報を読み取る位置情報読み取り手段と、

前記マーキングの現実の位置に関する情報を読み取るマーキング読み取り手段と、

前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とを利用して、それらを比較判定する比較判定手段と、

前記比較判定手段の比較判定結果に基づいて、前記光ディスクの記録データを再生する再生手段と、
を備えたことを特徴する再生装置。

14. 少なくとも前記出力された位置情報又はその位置情報に関する情報は、位置情報書き込み手段により前記ディスクに書き込まれていることを特徴する請求項13記載の再生装置。

15. 前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報を暗号化する暗号化手段を有し、

前記位置情報読み取り手段は、前記暗号化手段に対応する復号化手段を有し、
前記位置情報読み取り手段は、前記暗号化された位置情報又はその位置情報に関する情報を前記復号化手段により復号化することを特徴する請求項14記載の再生装置。

16. 前記暗号化手段は、前記暗号化する場合に、公開鍵系暗号関数の秘密鍵を用い、

前記復号化手段は、前記秘密鍵に対応する公開鍵を用いて、前記復号化を行うことを特徴する請求項15記載の再生装置。

17. 前記暗号化手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と
公開鍵系暗号関数のサブ公開鍵とを、前記公開鍵系暗号関数のマスタ秘密鍵により暗号化する第1暗号化手段と、

前記位置情報又はその位置情報に関する情報を前記サブ公開鍵に対応するサブ秘密鍵により暗号化する第2暗号化手段とを有し、

前記復号化手段は、

前記マスタ秘密鍵に対応するマスタ公開鍵により前記暗号化されたソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを復号化する第1復号化手段と、

その復号化されたサブ公開鍵を用いて、前記暗号化された位置情報又はその位置情報に関する情報を復号化する第2復号化手段と、

を有していることを特徴とする請求項15記載の再生装置。

18. 前記位置情報書き込み手段は、少なくとも前記出力された位置情報又はその位置情報に関する情報についてデジタル署名を行うデジタル署名手段を有し、そのデジタル署名を行った結果に関する情報を前記ディスクに書き込み、前記位置情報読み取り手段は、

前記デジタル署名手段に対応する認証手段と、

その認証手段による認証過程から、及び／又は前記デジタル署名結果に関する情報から前記位置情報を得る位置情報抽出手段とを有し、

前記比較判定手段は、前記認証手段により前記認証結果が正常である旨の出力がされた場合は、前記位置情報抽出手段により得られた位置情報と、前記マーキング読み取り手段による読み取り結果とを利用して、前記比較判定を行い、又、前記正常である旨の出力がされない場合は、前記再生を行わないことを特徴する請求項14記載の再生装置。

19. 前記デジタル署名手段は、前記デジタル署名する場合に、公開鍵系暗号関数の秘密鍵を用い、

前記認証手段は、前記秘密鍵に対応する公開鍵を用いて、前記認証を行うことを特徴する請求項18記載の再生装置。

20. 前記デジタル署名手段は、

ディスクに書き込まれるソフト内容の特徴に関するソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とについて、前記公開鍵系暗号関数のマスタ秘密鍵によりデジタル署名する第1デジタル署名手段と、

前記位置情報又はその位置情報に関する情報について、前記サブ公開鍵に対応するサブ秘密鍵によりデジタル署名する第2デジタル署名手段とを有し、

前記少なくとも前記出力された位置情報又はその位置情報に関する情報を書き込むとは、

前記第1デジタル署名手段によるデジタル署名を行った結果に関する情報と、前記第2デジタル署名手段によるデジタル署名を行った結果に関する情報とを前記ディスクに書き込むことであり、

前記位置情報読み取り手段は、

前記マスタ秘密鍵に対応するマスタ公開鍵により前記デジタル署名された、ソフト特徴情報と公開鍵系暗号関数のサブ公開鍵とを認証する認証手段と、

その認証過程から、及び／又は前記デジタル署名結果から得られたサブ公開鍵を用いて、前記認証過程から、及び／又は前記デジタル署名結果から前記位置情報を得る位置情報抽出手段とを有し、

前記比較判定手段は、前記認証手段により前記認証結果が正常である旨の出力がされた場合は、前記位置情報抽出手段により得られた位置情報と、前記マーキング読み取り手段による読み取り結果とを利用して、前記比較判定を行い、又、前記正常である旨の出力がされない場合は、前記再生を行わないことを特徴とする請求項18記載の再生装置。

21. 前記比較判定の結果、前記位置情報読み取り手段による読み取り結果と、前記マーキング読み取り手段による読み取り結果とが相互に一致しない場合には、前記再生を行わないことを特徴する請求項13～20の何れか一つに記載の再生装置。

22. 前記公開鍵系暗号関数は、RSA関数又は楕円関数であることを特徴する請求項16、17、19又は20に記載の再生装置。

23. ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜に対してマーキングを施すステップと、

前記マーキングの位置を検出するステップと、

前記検出された位置をマーキングの位置情報として出力し、暗号化して前記ディスクに書き込むステップと、

を備えたことを特徴する光ディスク製造方法。

24. ディスクの成形を行うステップと、

前記成形されたディスクに反射膜を形成するステップと、

前記反射膜に対してマーキングを施すステップと、

前記マーキングの位置を検出するステップと、

前記検出された位置をマーキングの位置情報として出力し、その位置情報に関連してデジタル署名して前記ディスクに書き込むステップと、

を備えたことを特徴する光ディスク製造方法。

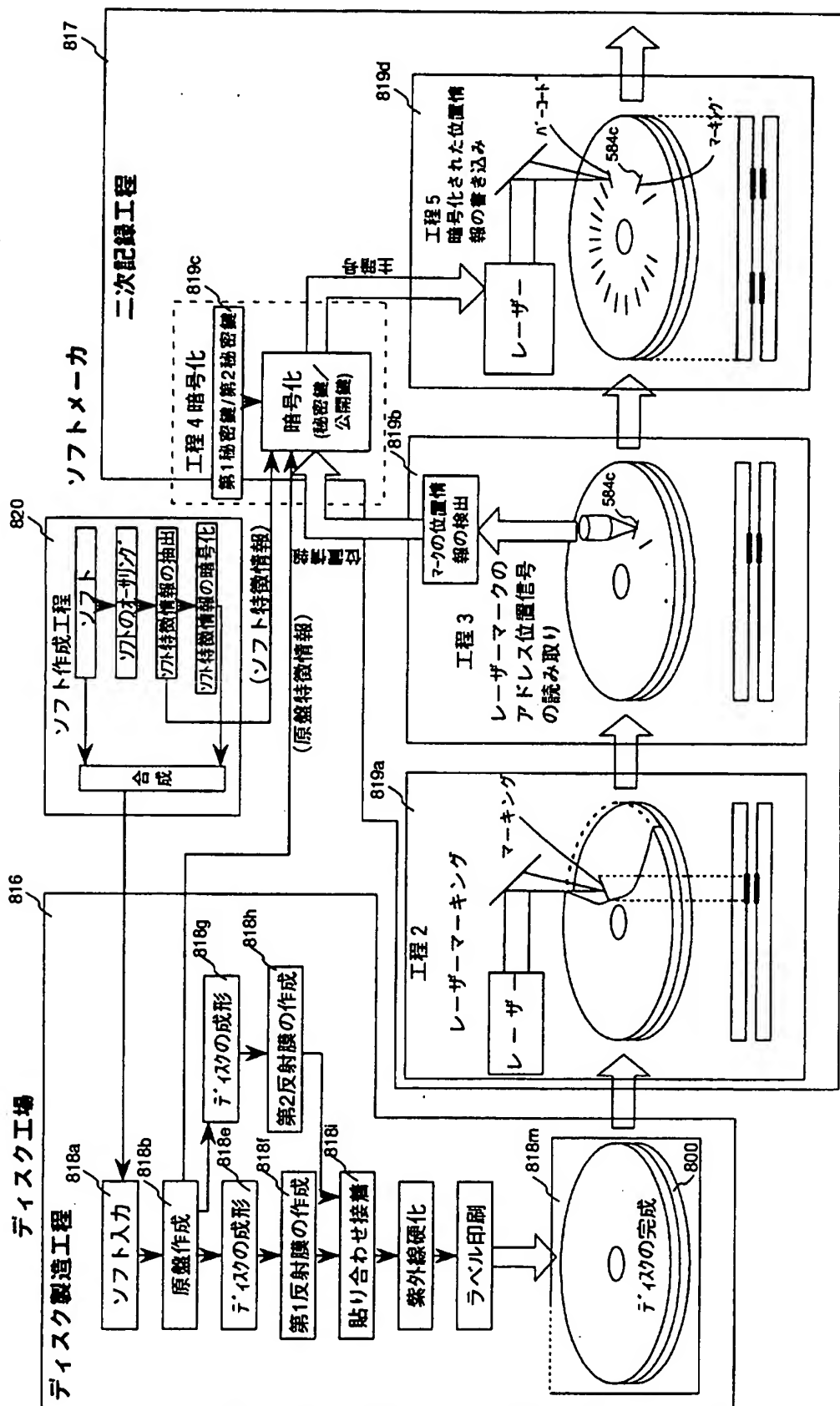
25. データの書き込まれたディスクの反射膜にレーザーによりマーキングが施されており、少なくともそのマーキングの位置情報又はその位置情報に関する情報が、暗号化され、あるいはデジタル署名された形で、前記ディスクに書き

込まれていることを特徴とする光ディスク。

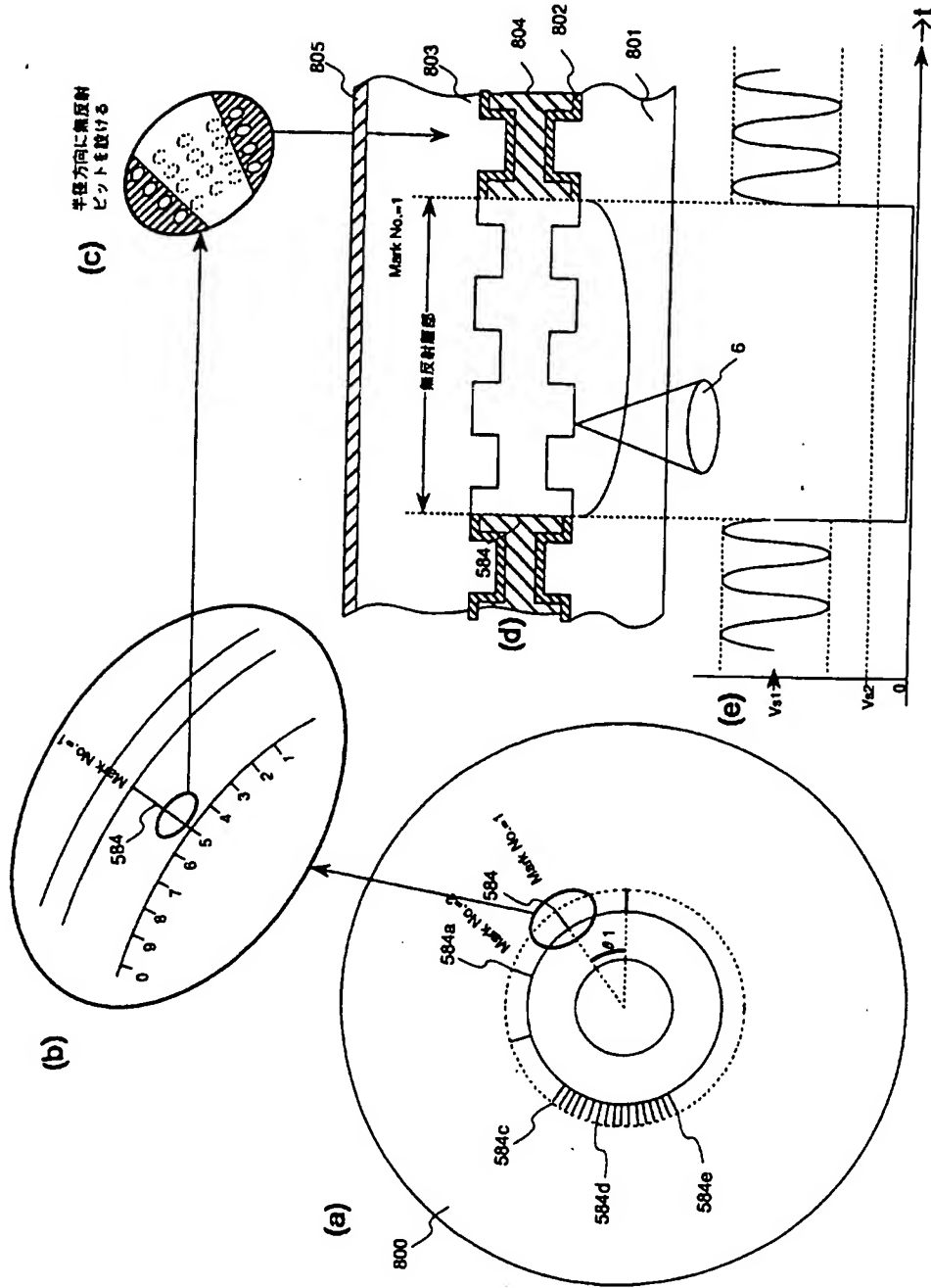
26. レーザにより消滅しない材料からなる2つの部材により反射膜が直接又は間接的に挟まれた構造を備えたディスクであって、その反射膜にレーザーによりマーキングが施されていることを特徴とする光ディスク。

27. ソフトコンテンツの特徴を、情報特徴抽出手段もしくは情報圧縮手段により、特徴抽出したソフト特徴情報と、前記ソフトコンテンツが海賊版防止もしくはコピー防止の対象ソフトであるか否かを示す海賊版防止識別子もしくはコピー防止識別子とを、一括して公開鍵系暗号関数の秘密鍵を用いてデジタル署名処理を行った結果の署名データが、前記ソフトコンテンツとともに、同一媒体上に記録されていることを特徴とする光ディスク。

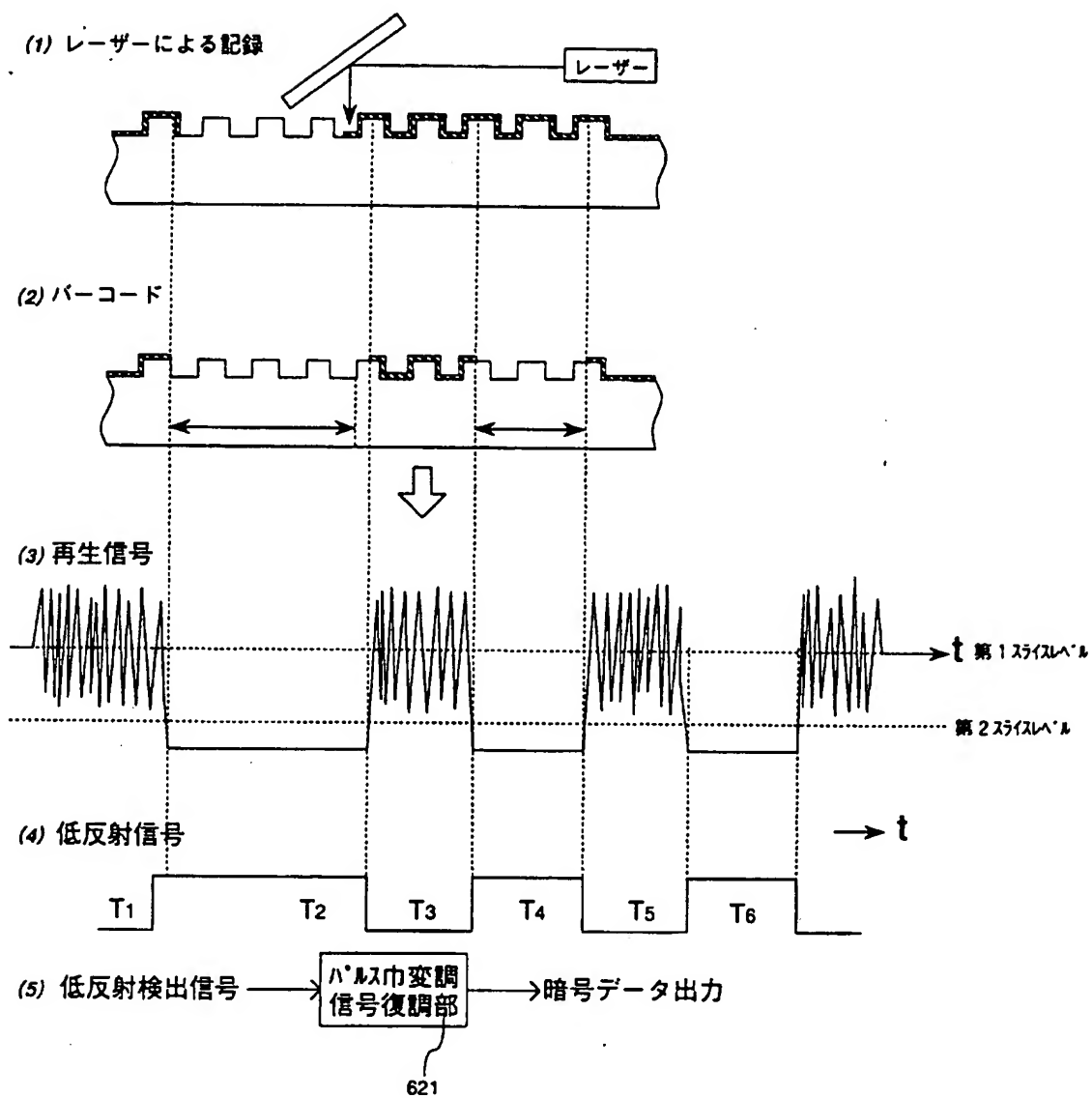
第1図



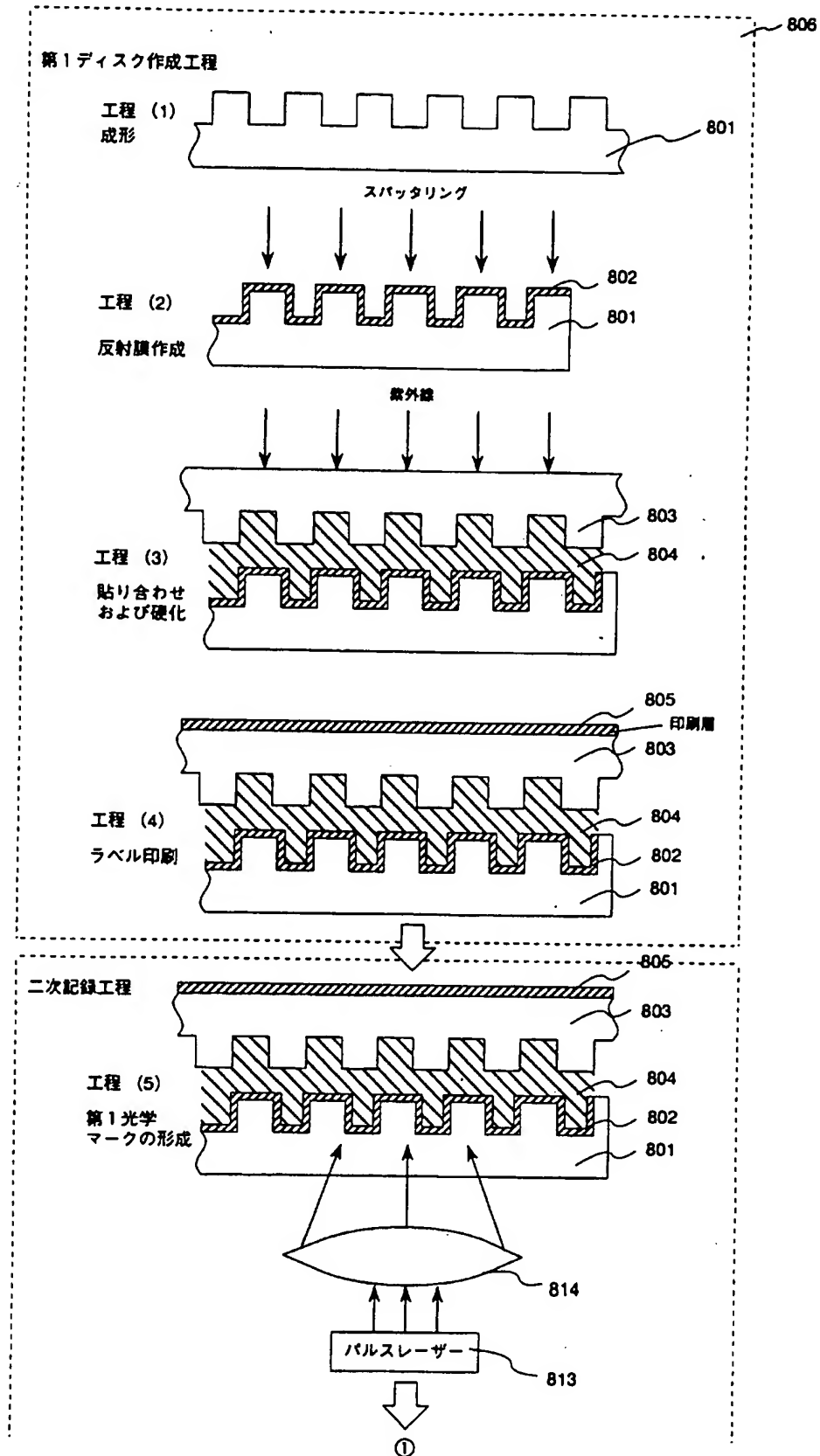
第2図



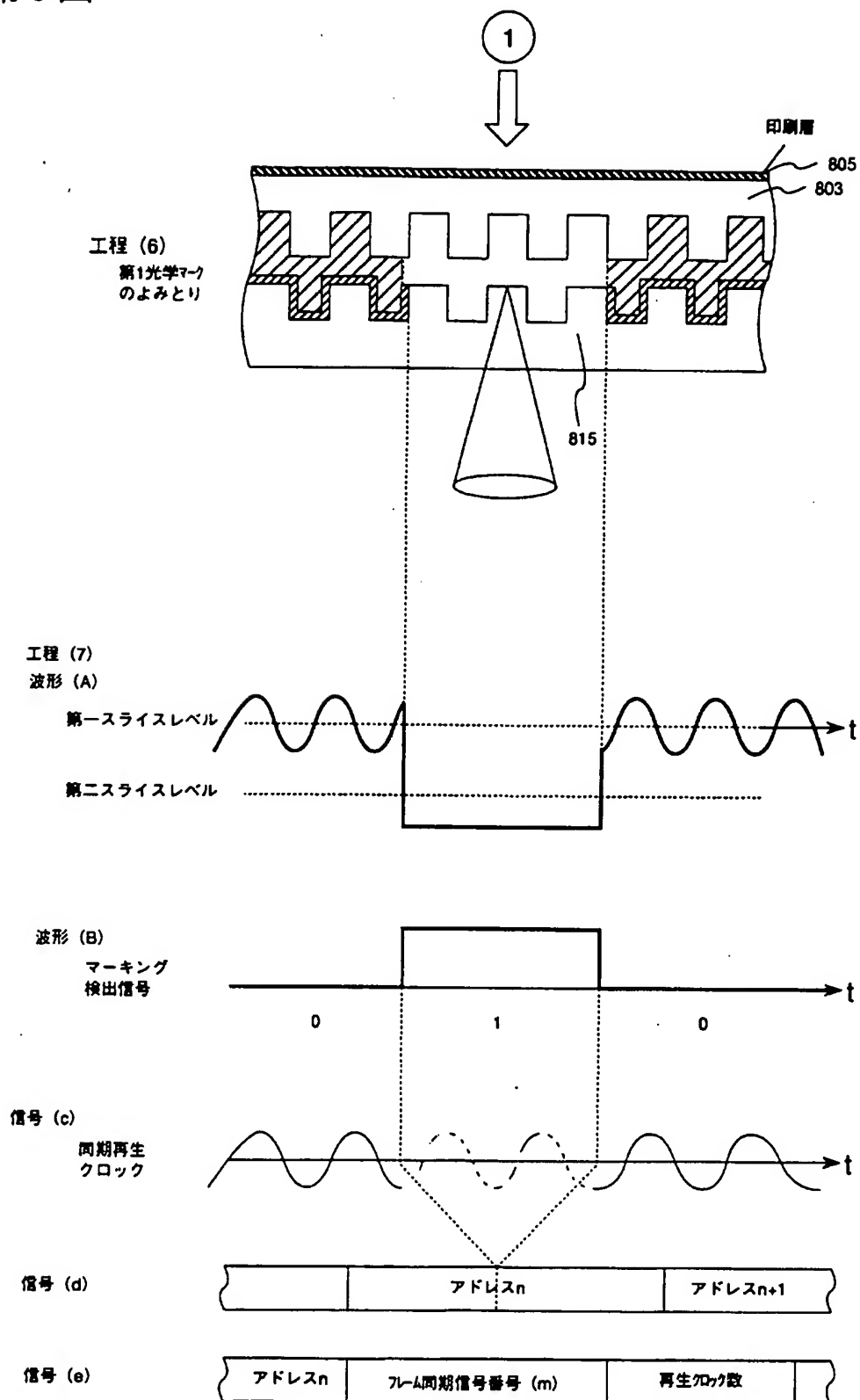
第3図



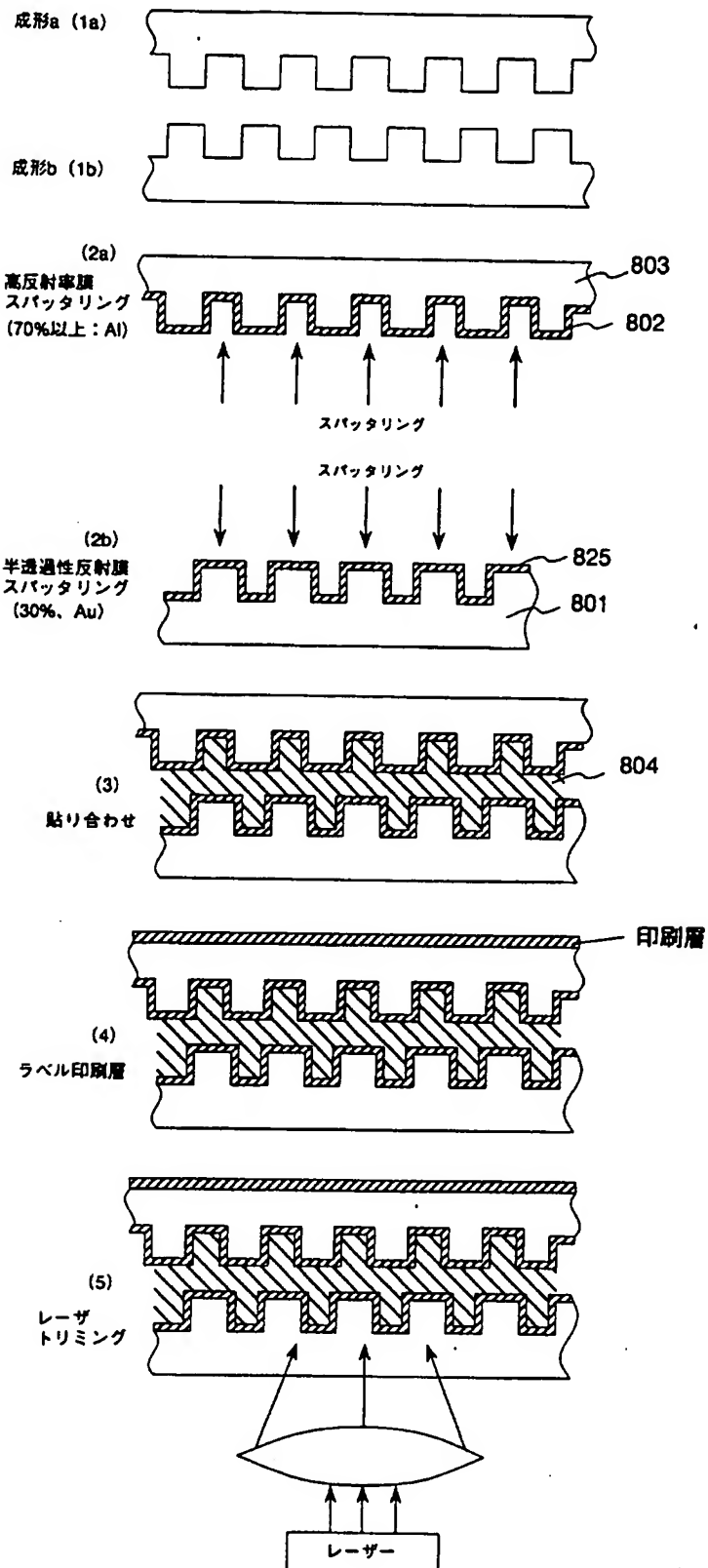
第4図



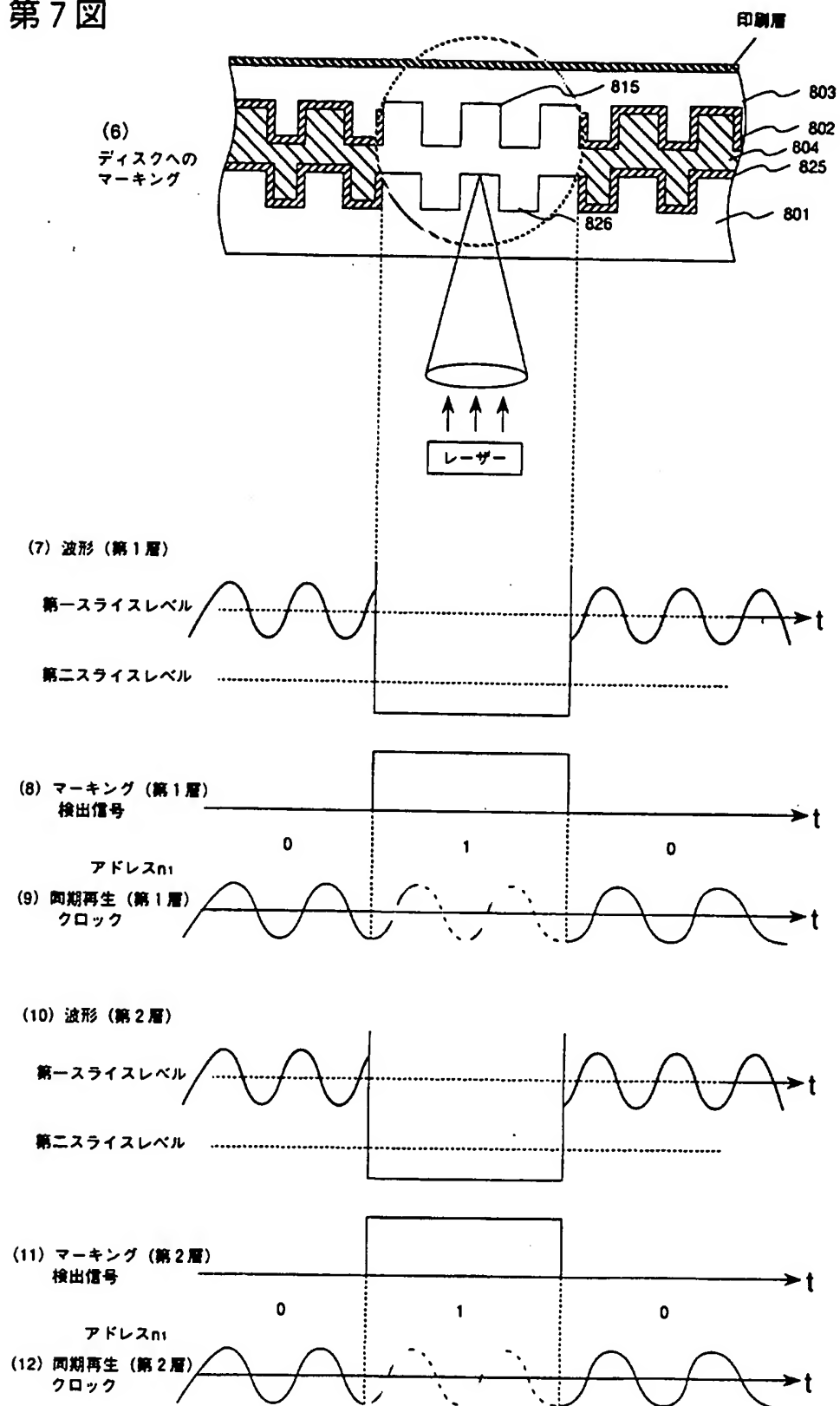
第5図



第6図

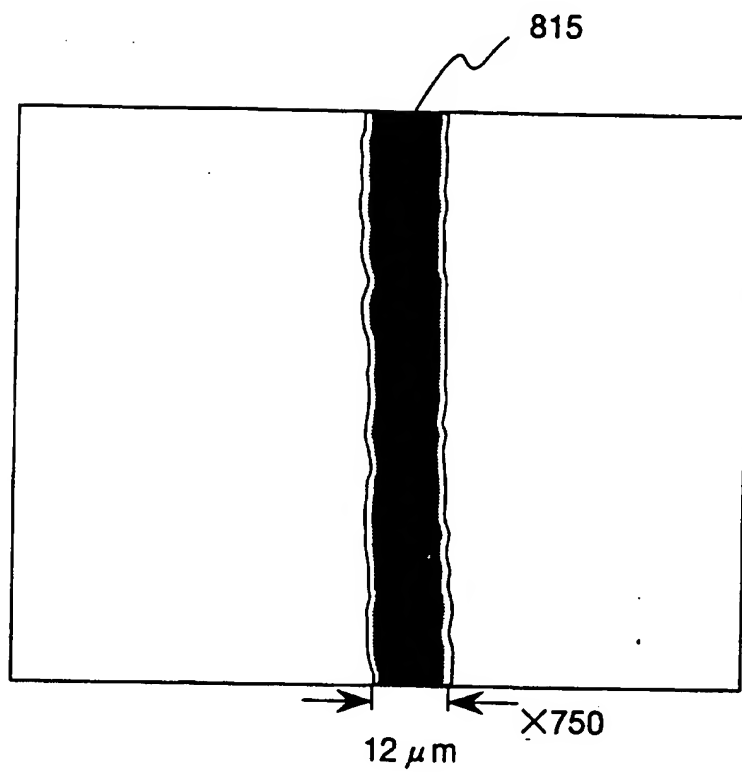


第7図

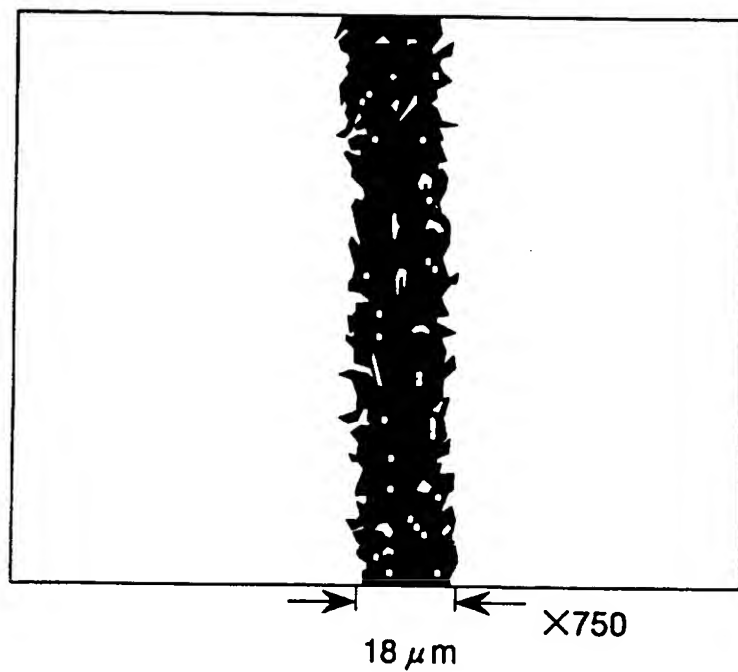


第 8 図

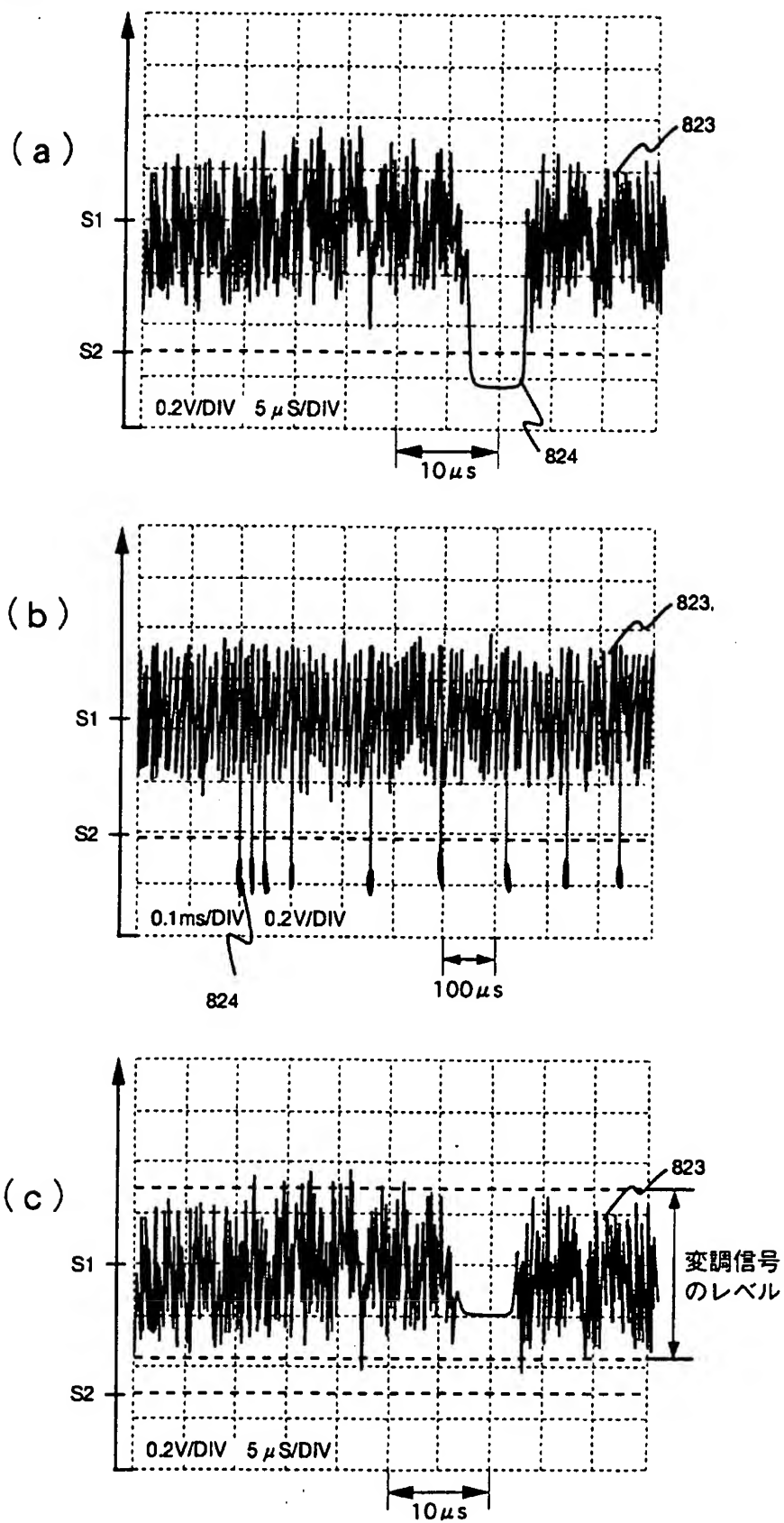
(a)



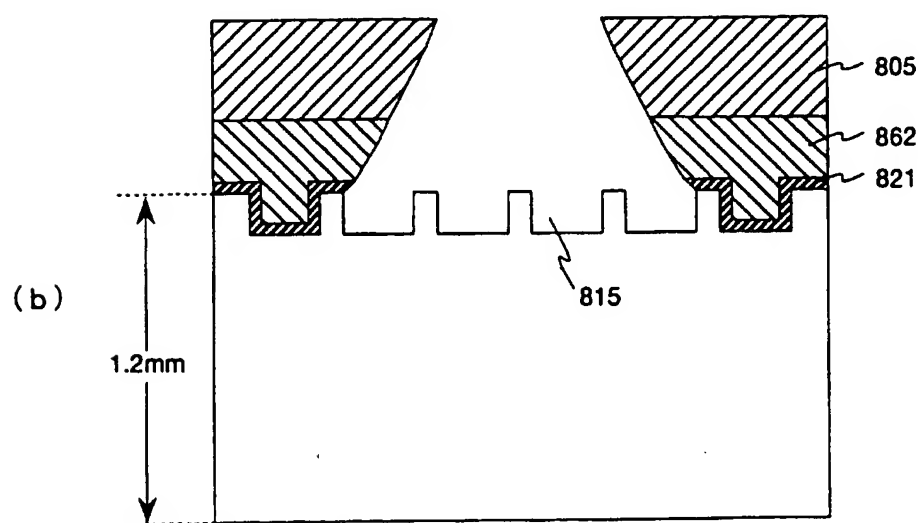
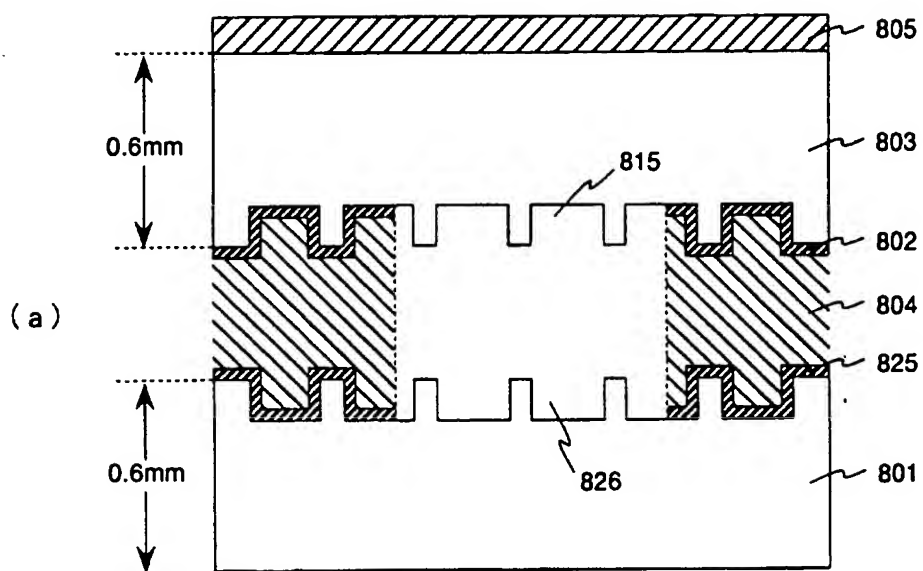
(b)



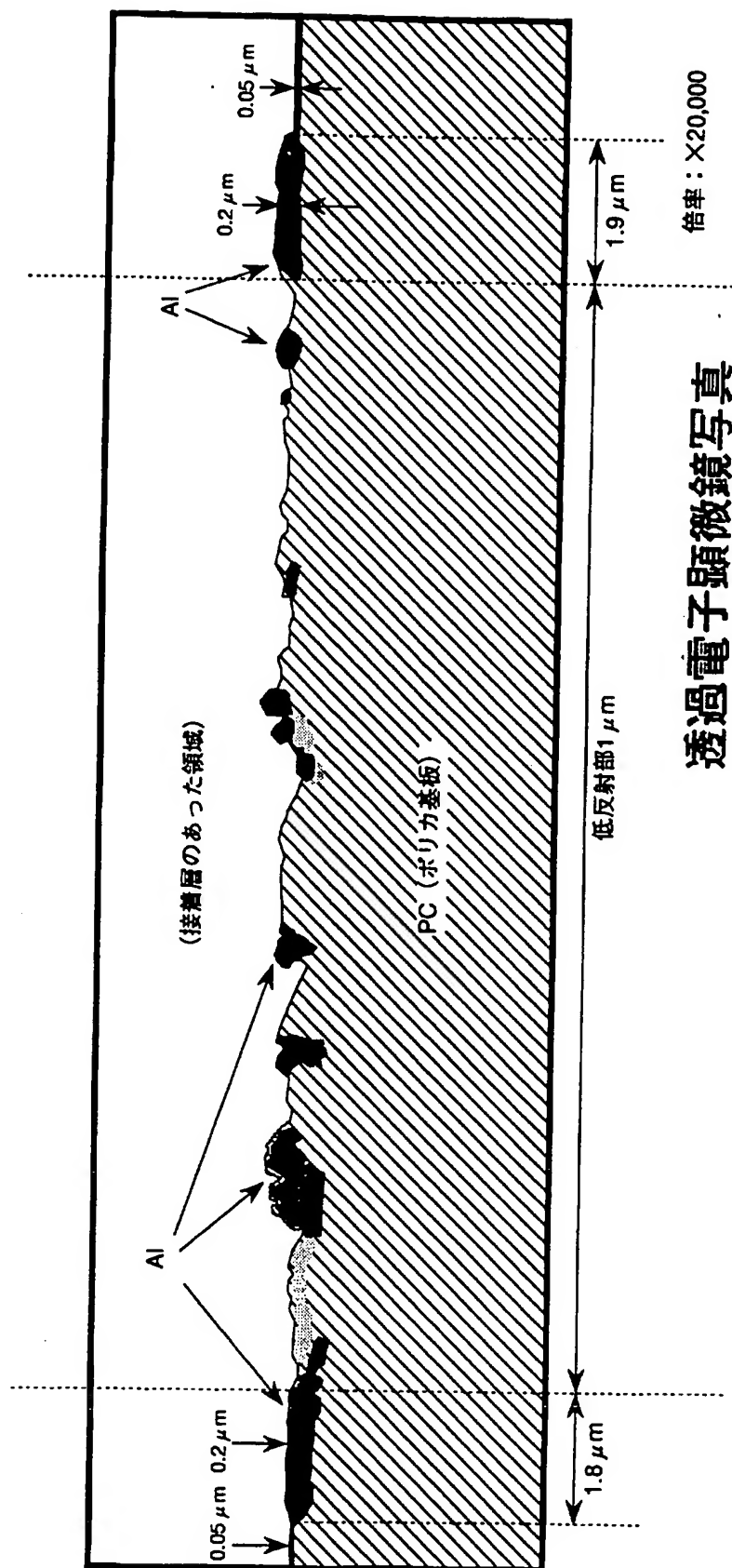
第9図



第 10 図

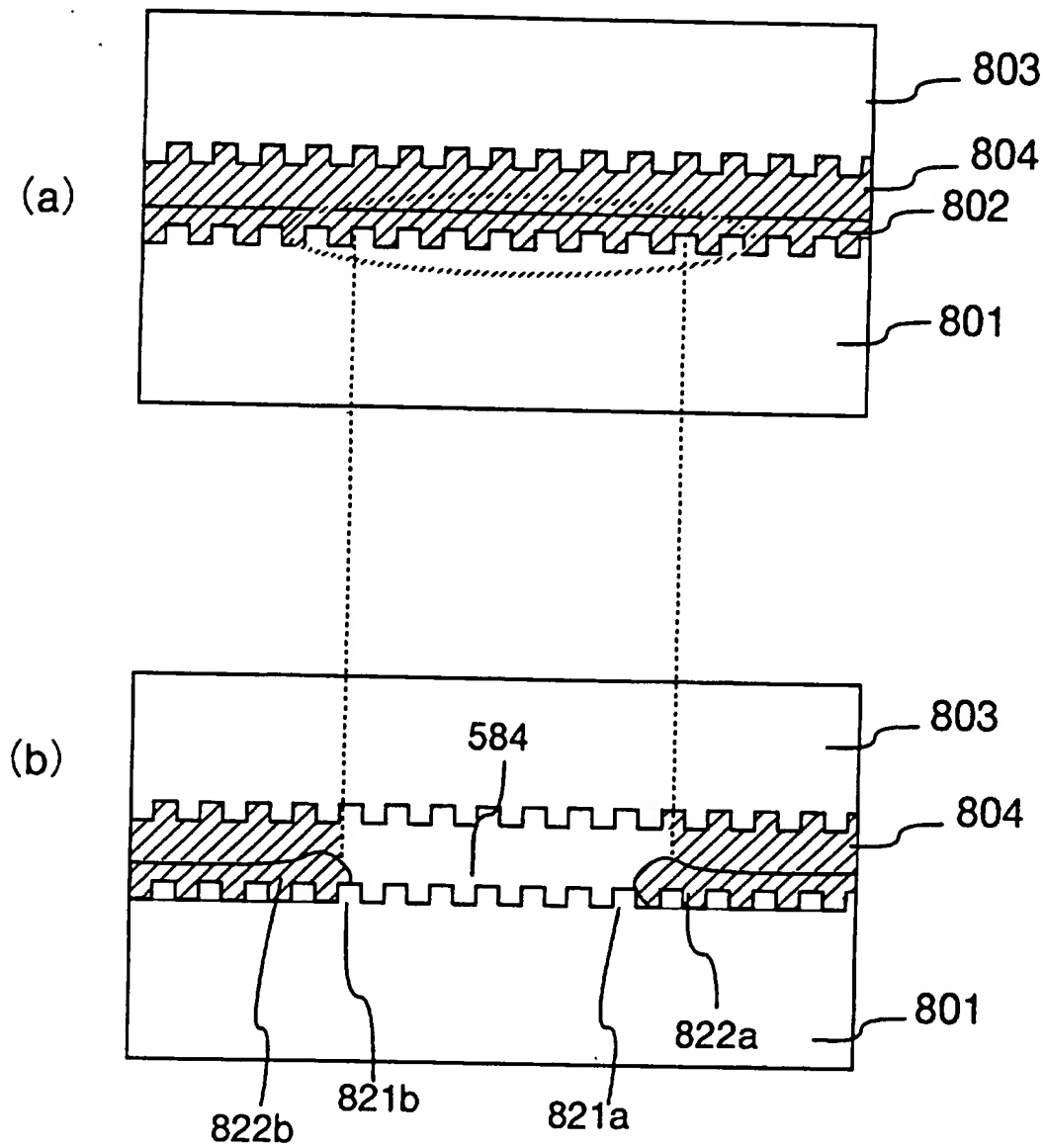


第11図

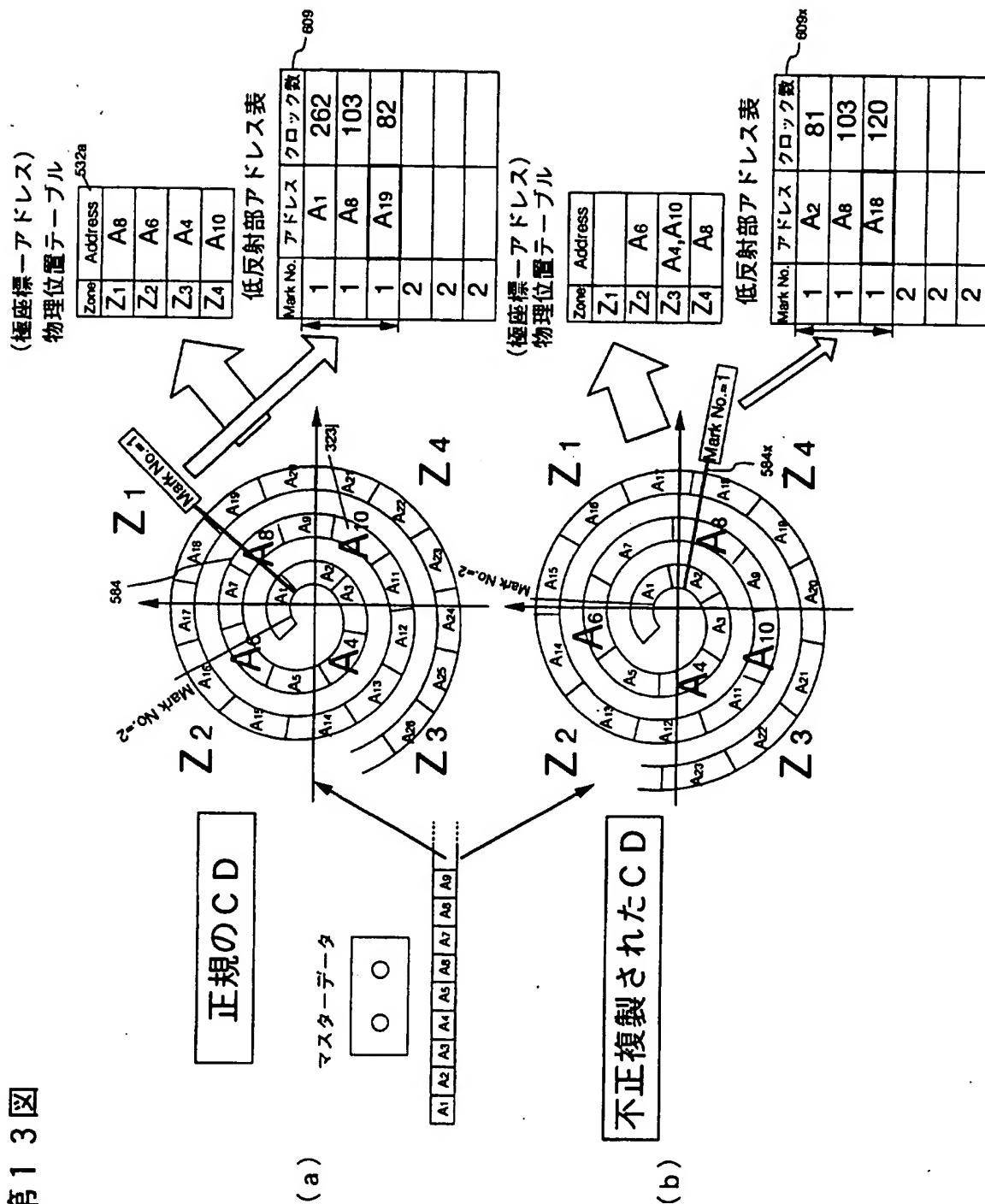


透過電子顕微鏡写真

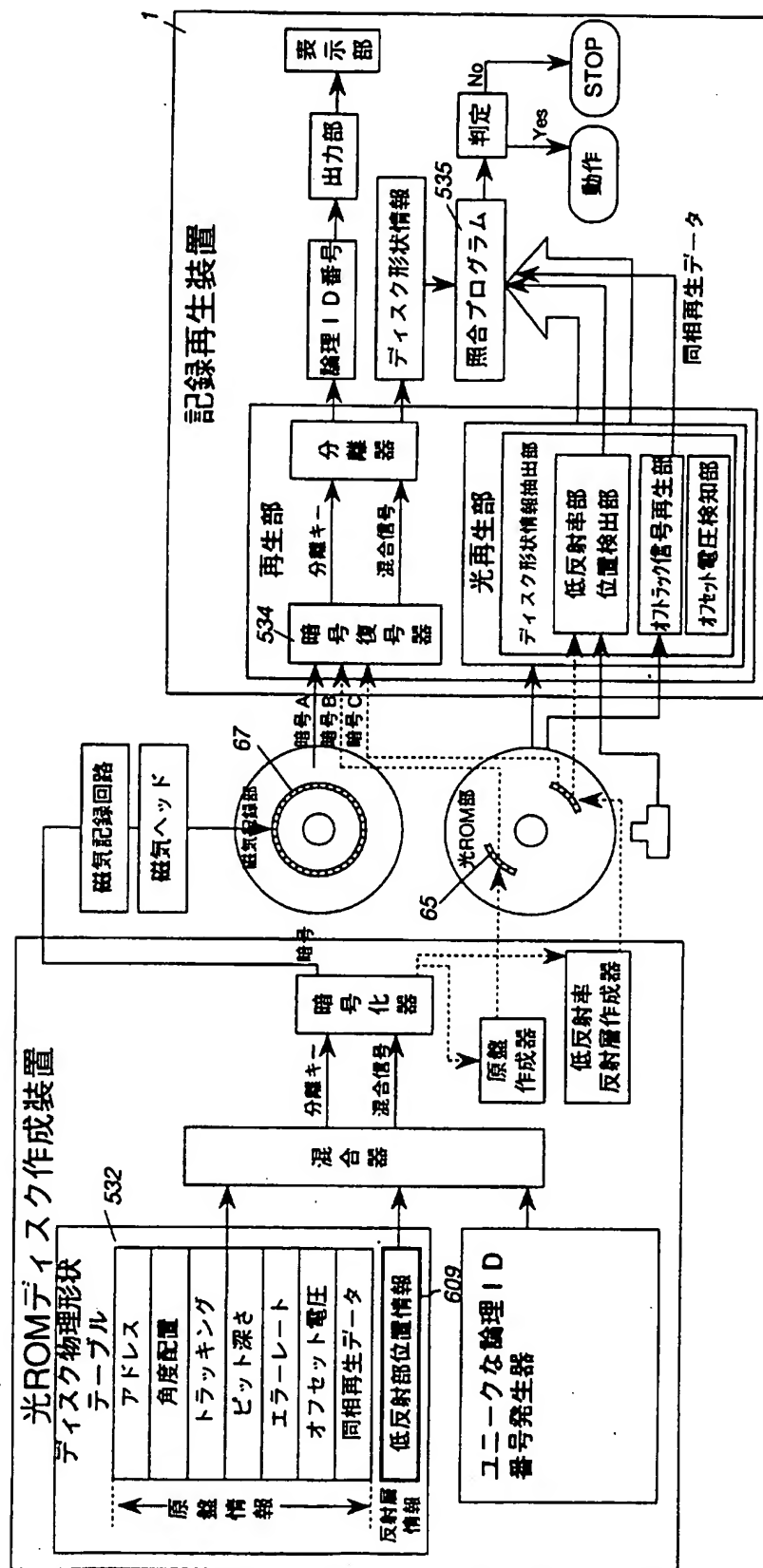
第 1 2 図



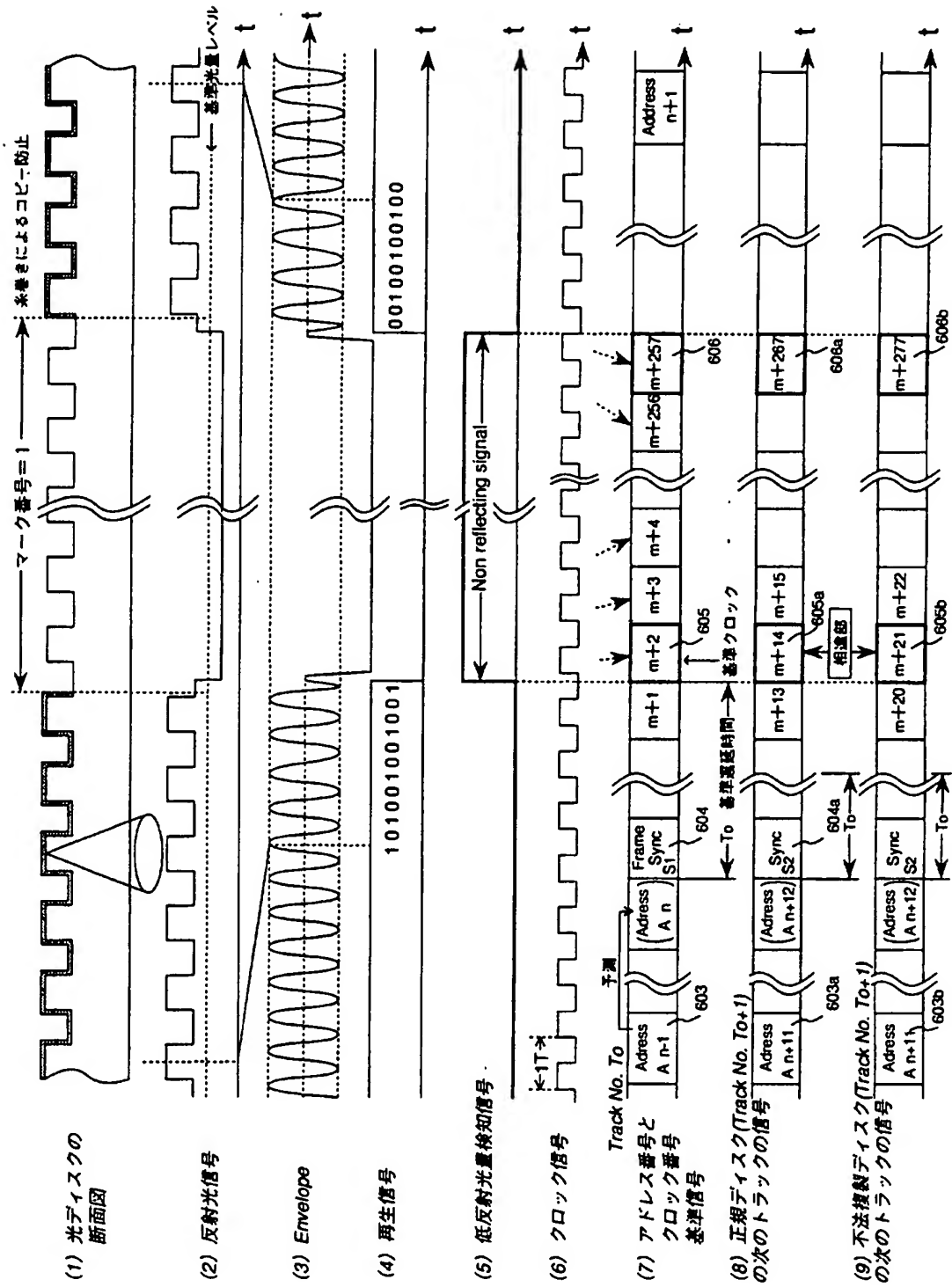
第13図



第14図



第16図



第17図

正規のディスク

低反射部 - アドレステーブル

マ-クNo.	開始位置			終了位置		
	アドレス	Sync No	加-マ番号	アドレス	Sync No	加-マ番号
1	A n	S1	m+2	n		m+257
1	A n+12	S2	m+14	n+12		m+267
1	A n+23		m+25	n+23		m+300
:	:		:	:		:
2	A n+1		m+15	n+1		m+160
2	A n+13		m+85	n+13		m+250
2	A n+24		m+68	n+24		m+210
10	A n+9					
10						

比較

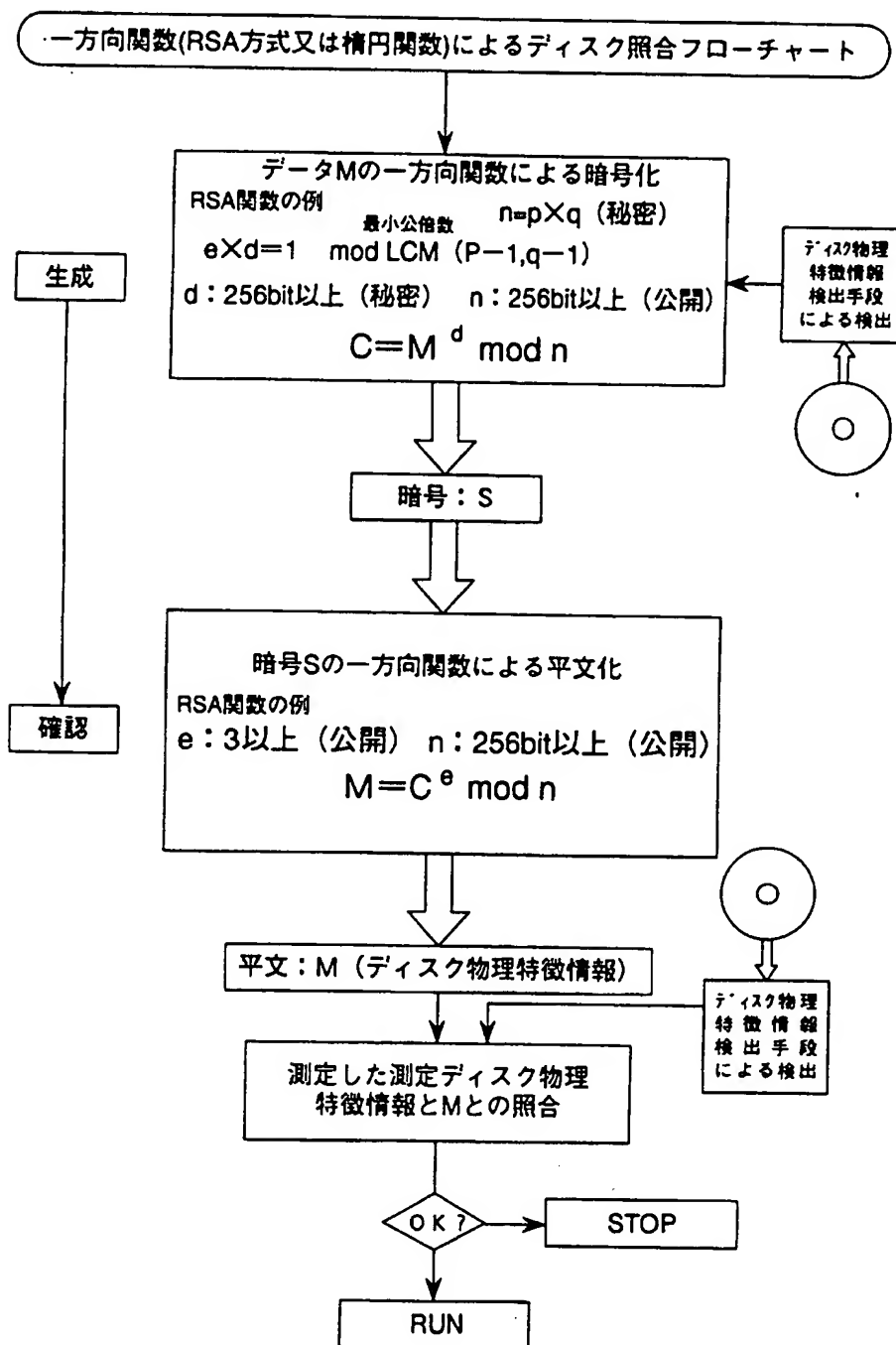
不正複製されたディスク

低反射部 - アドレステーブル

マ-クNo.	開始位置			終了位置		
	アドレス	Sync No	加-マ番号	アドレス	Sync No	加-マ番号
1	n	S1	m+2	n		m+257
1	n+12	S2	m+21	n+12		m+277
1	n+22		m+4	n+22		m+230
:	:		:	:		:
2	n+1		m+36	n+1		m+190
2	n+13		m+120	n+13		m+281
2	n+25			n+25		
10	n+9					
10						

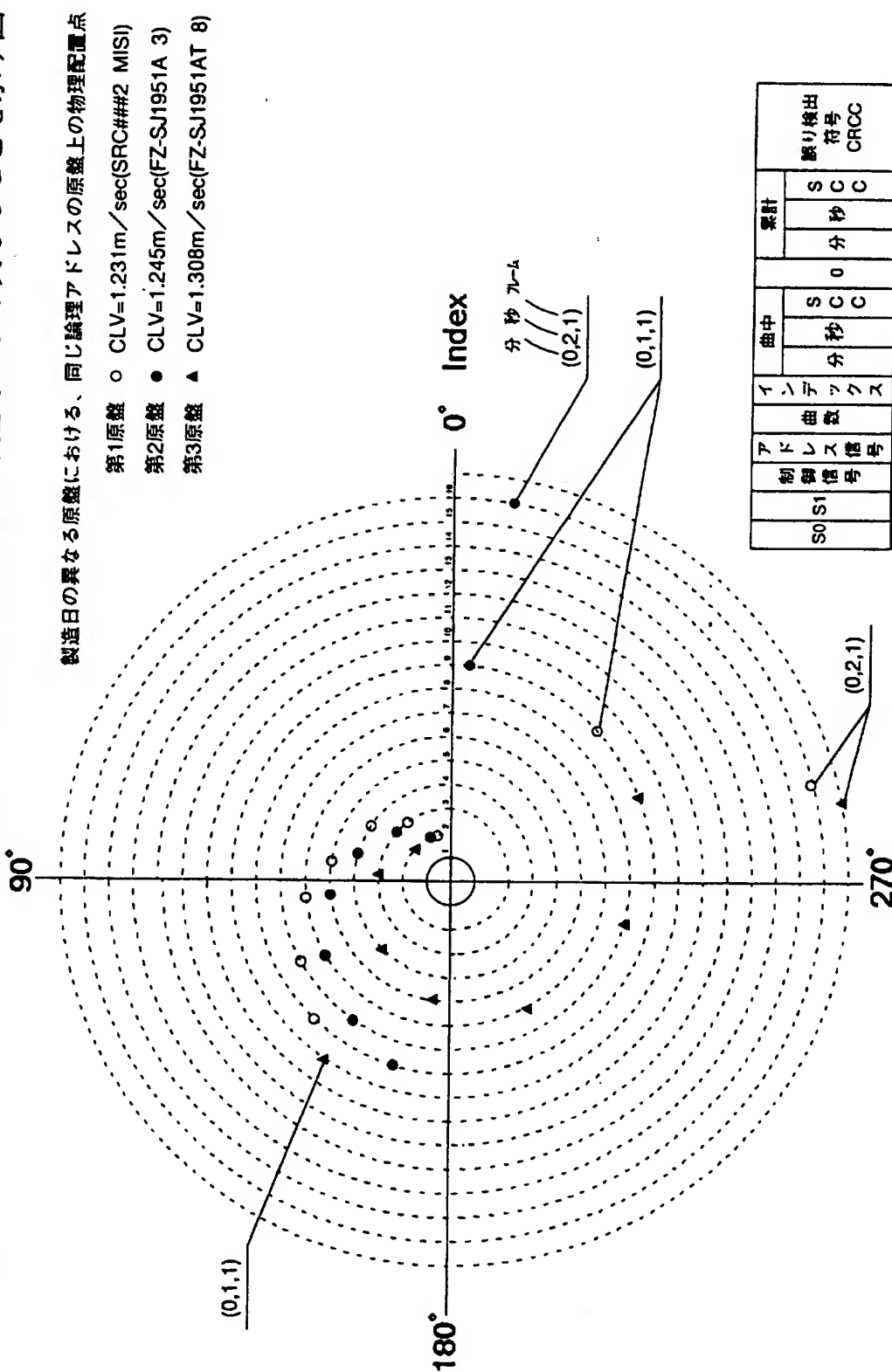
609x

第 18 図

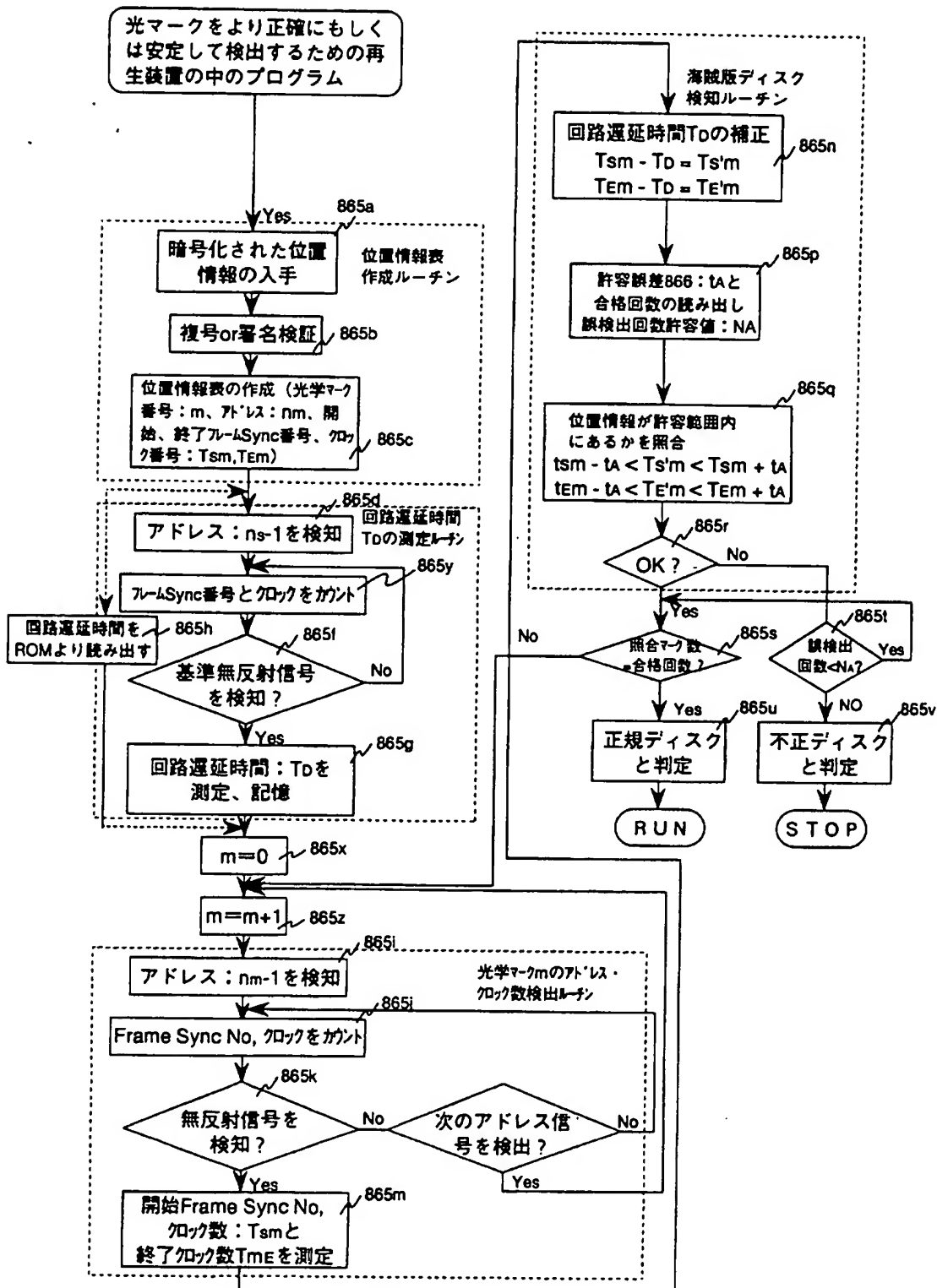


第19図

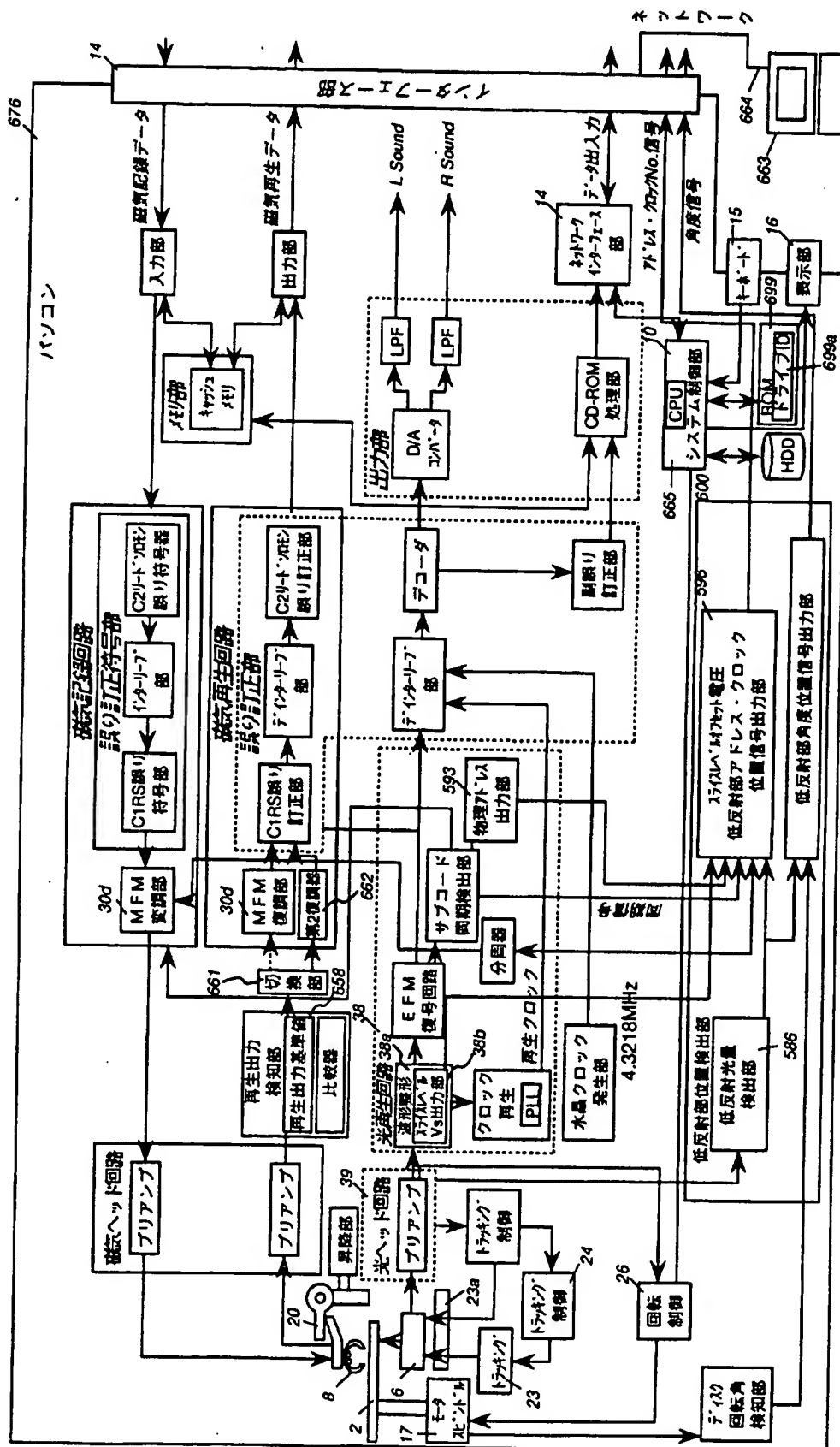
論理アドレスの物理的位置が原盤毎により異なることを示す図



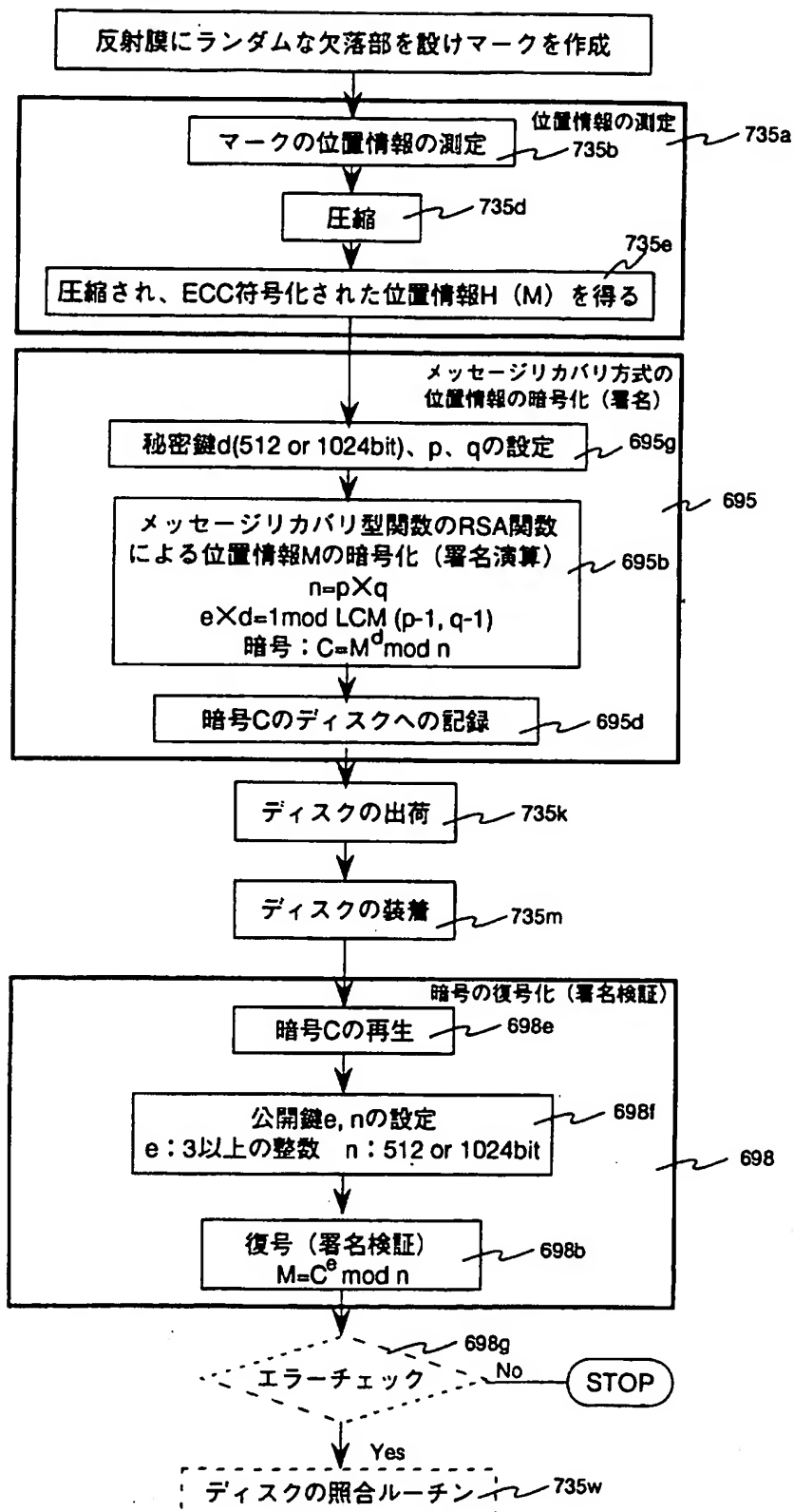
第20図



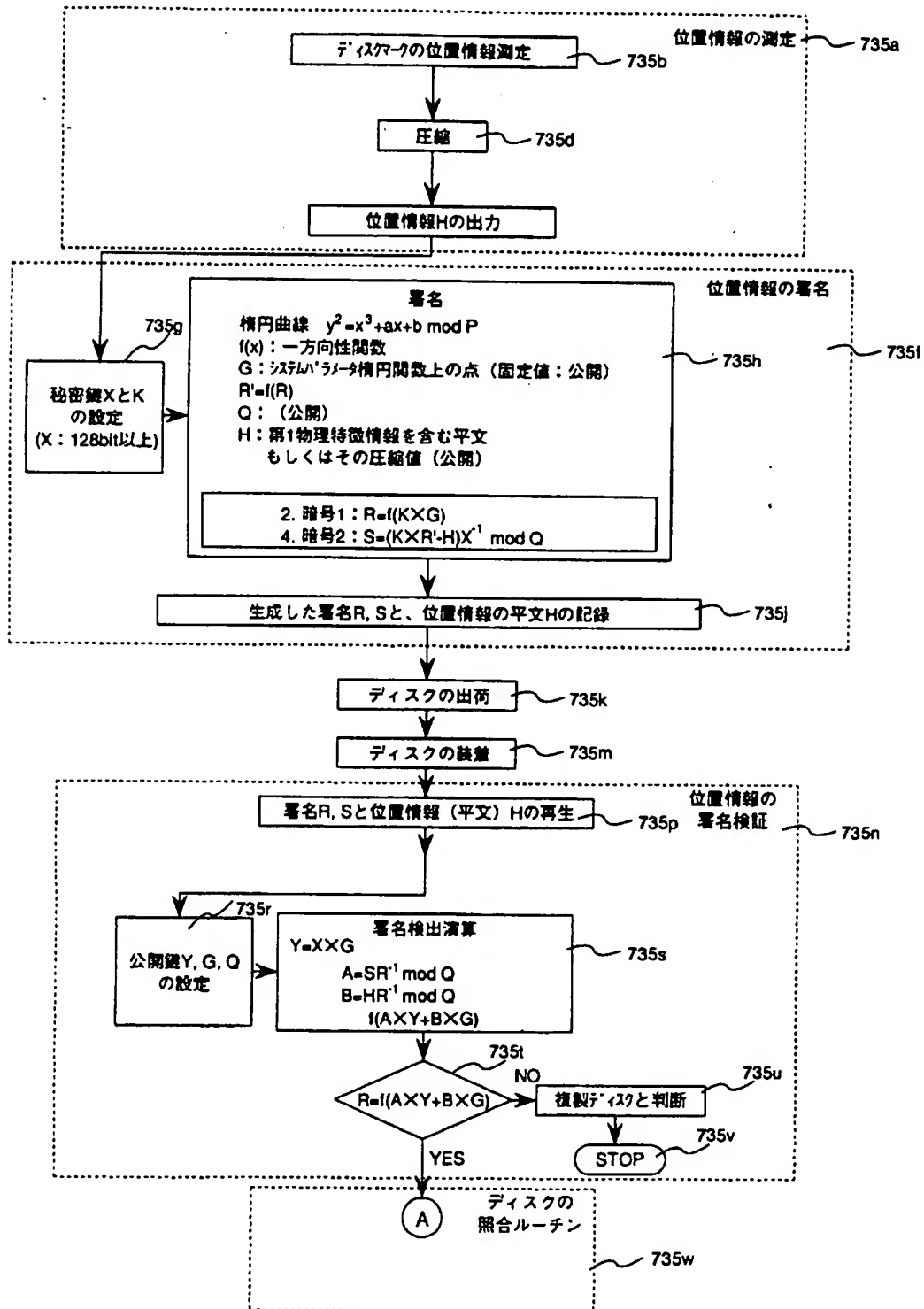
第21図



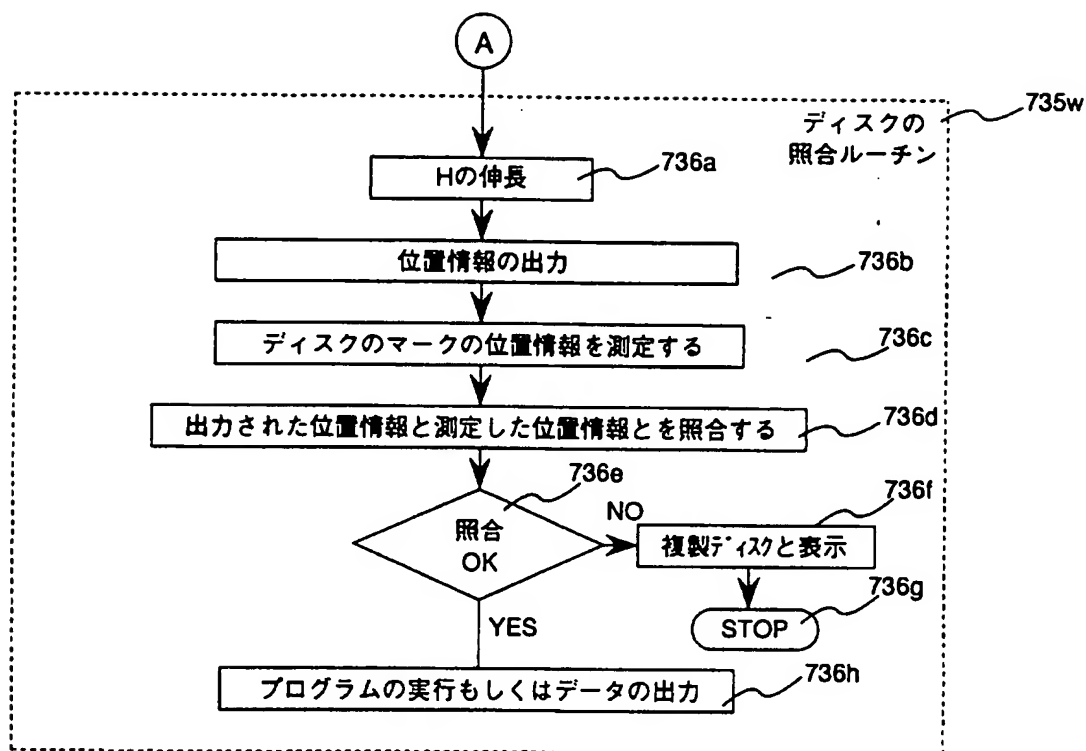
第 2 2 図



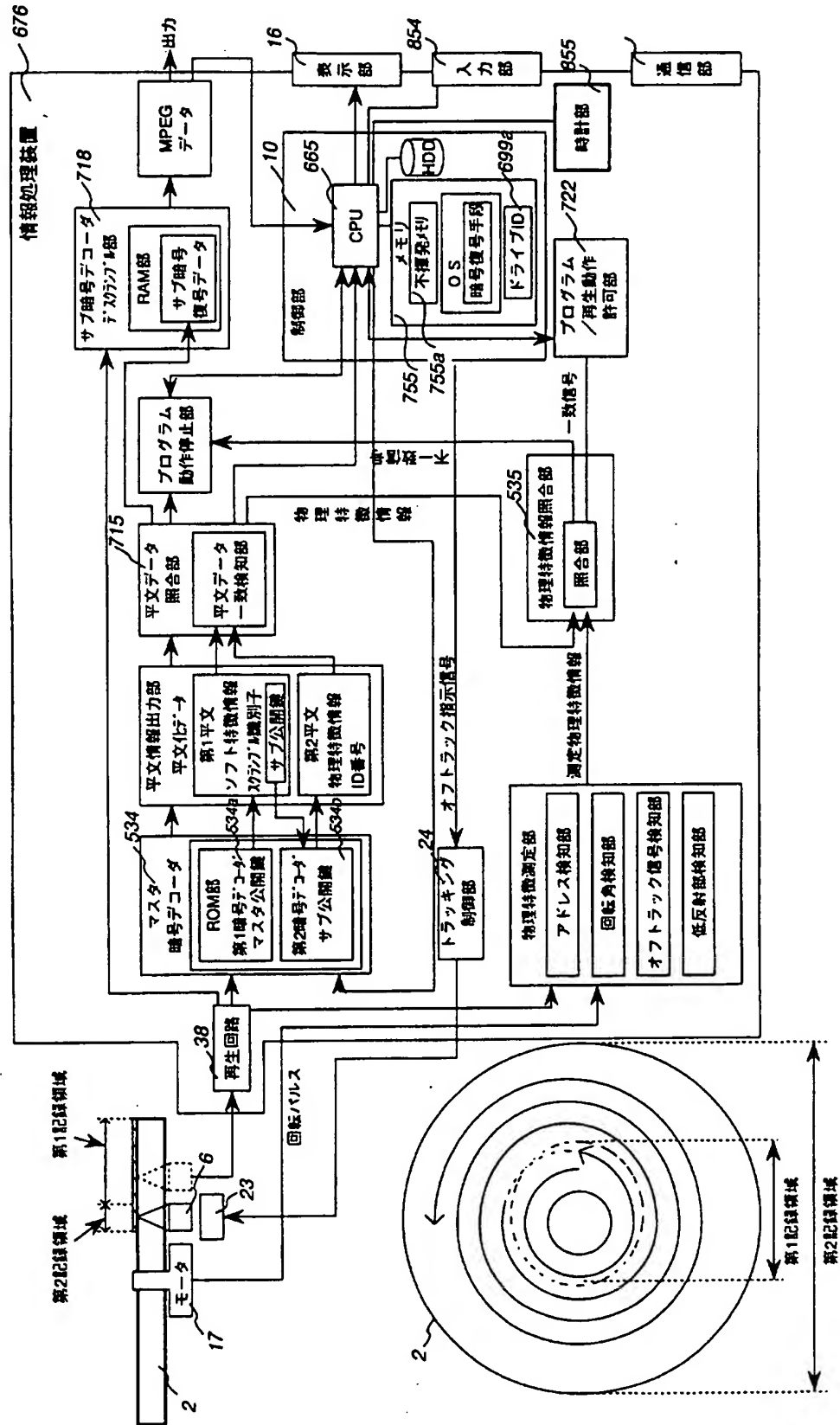
第 2 3 図



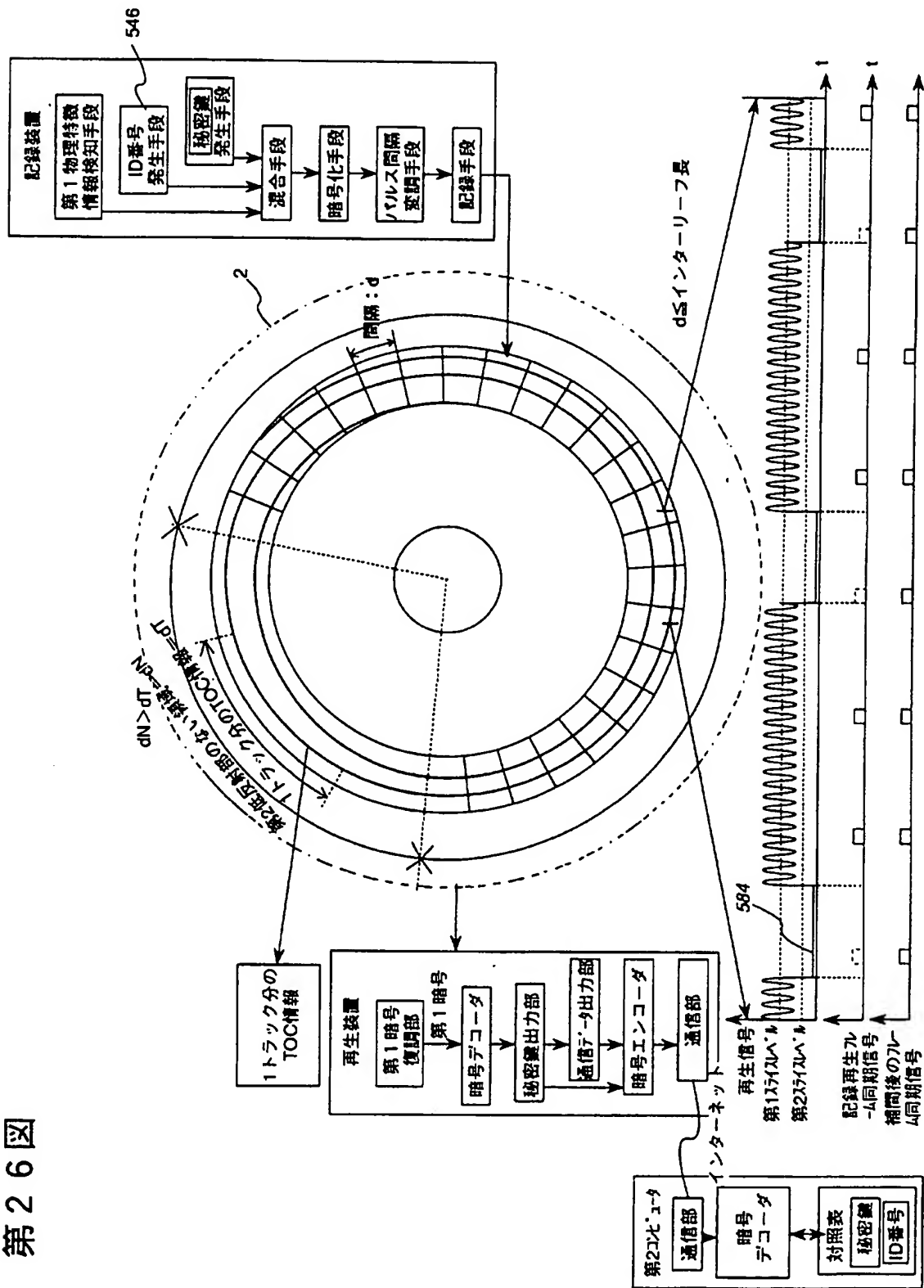
第 2 4 図



第25図



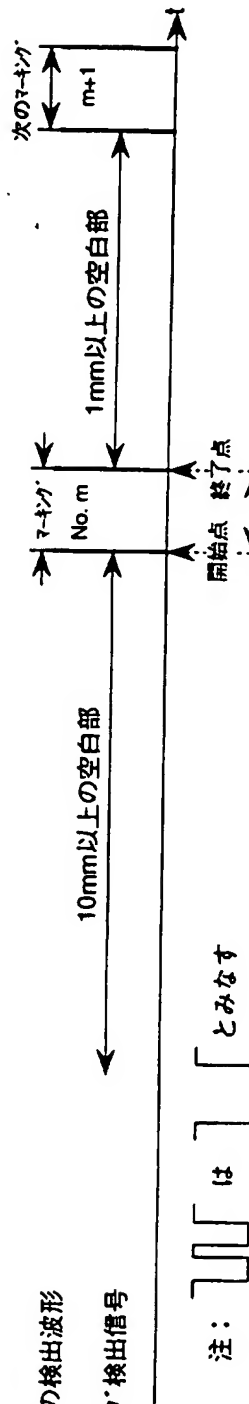
第26図



第27図

1層目のマーキング信号の検出波形

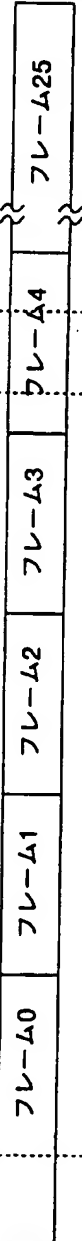
(1) 1層目のマーキング信号の検出波形



(2) アドレス



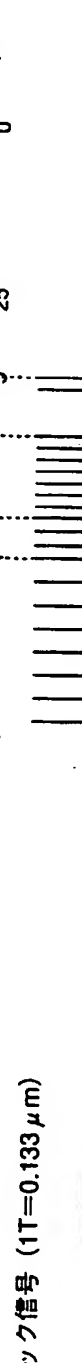
(3) フレーム位置



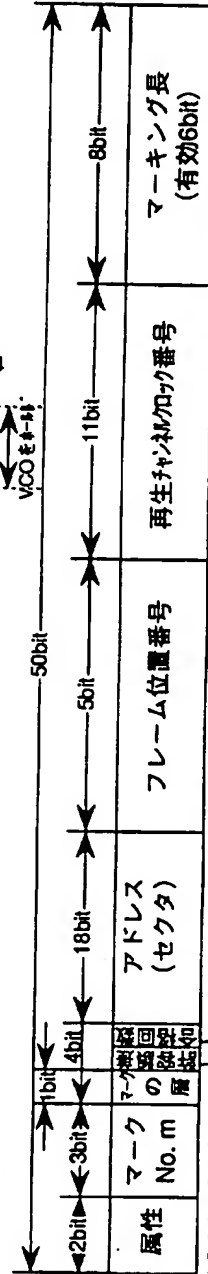
(4) フレーム同期信号



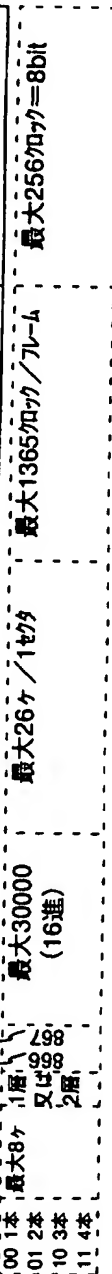
(5) PLL再生クロック信号 (1T=0.133 μm)



(6) マーキング位置データ



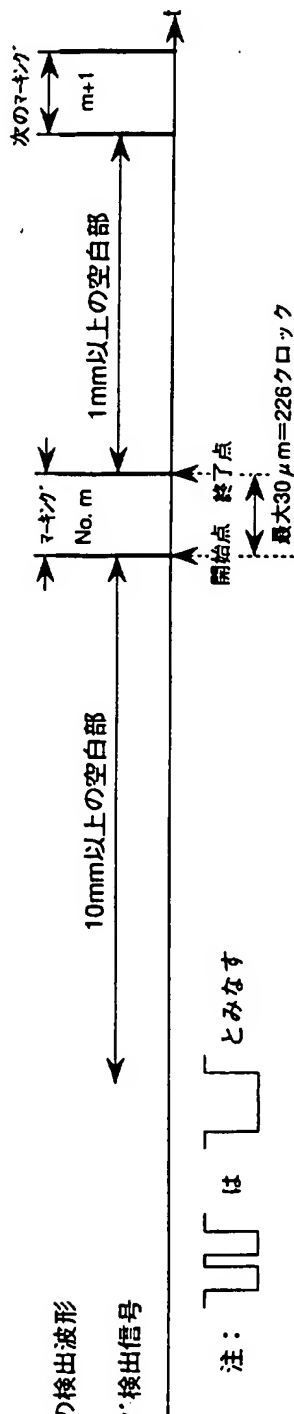
(7) データ例



第 28 図

2 層目のマーキング信号の検出波形

(1) 2 層目のマーキング検出信号

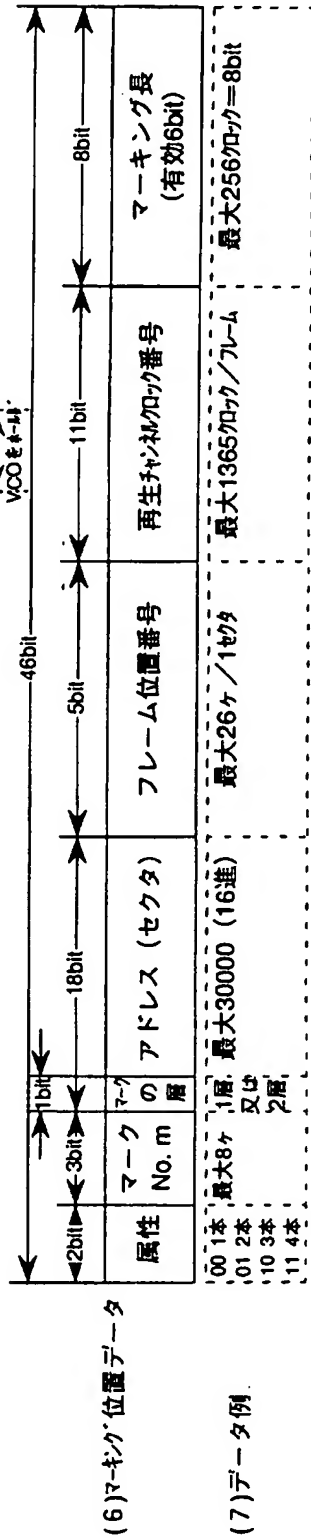


(2) 2 層目のアドレス アドレス (n+10) アドレス (n+11)

(3) フレーム位置 フレーム 0 フレーム 1 フレーム 2 フレーム 8 フレーム 9 フレーム 25

(4) フレーム同期信号

(5) PLL 再生クロック信号 ($1T = 0.133\mu m$)

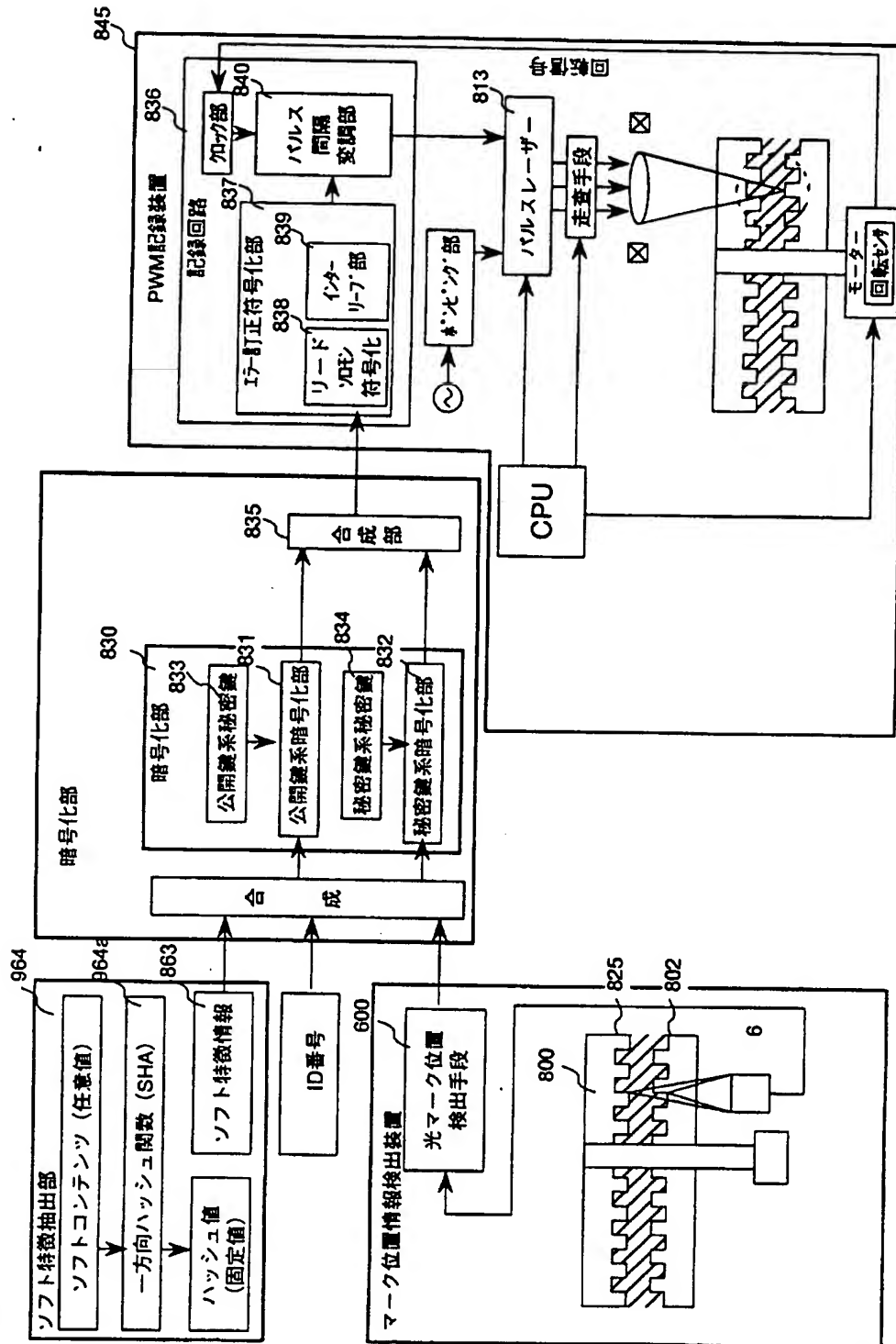


(6) マーキング位置データ

(7) データ例

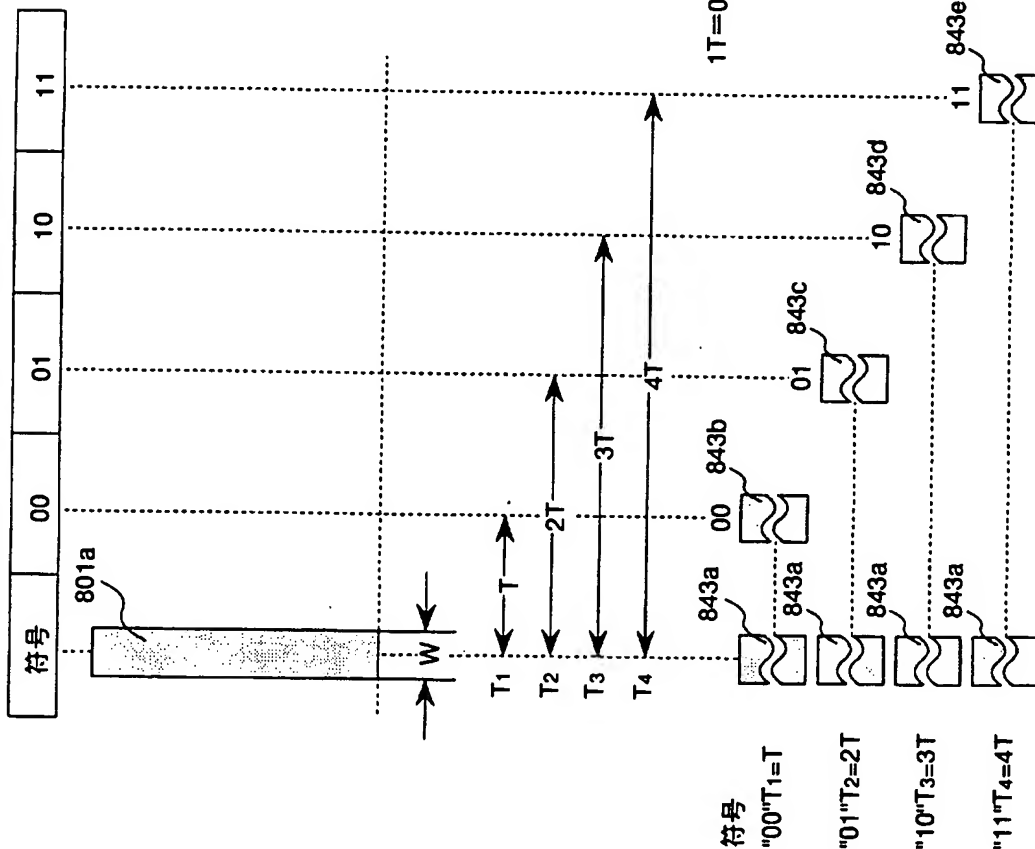
属性	マーキング No. m	マーキングの層	アドレス (セクタ)	フレーム位置番号	再生チャンネル/クロック番号	マーキング長 (有効 6bit)
00 1本	最大 8ヶ	1層	最大 30000 (16進)	最大 26ヶ / 1セクタ	最大 1365クロック / フレーム	最大 256クロック = 8bit
01 2本	又は					
10 3本	2層					
11 4本						

第29図



第 30 図

4値PWM記録の場合のパルス間隔別の符号



バーコードの線巾と記録密度の関係

線巾 $W (\mu m)$	周期 $T (\mu m)$	記録密度 $\mu m/bit$	最大記録容量 1周分	1Kbitの長さ mm
1	2	2.55	56Kbit	2.5mm
3	6	7.5	28.2Kbit	5mm
5	10	12.5	11.2Kbit	12.5mm
10	20	25	5.6Kbit	25mm
20	40	50	2.82Kbit	50mm

第31図

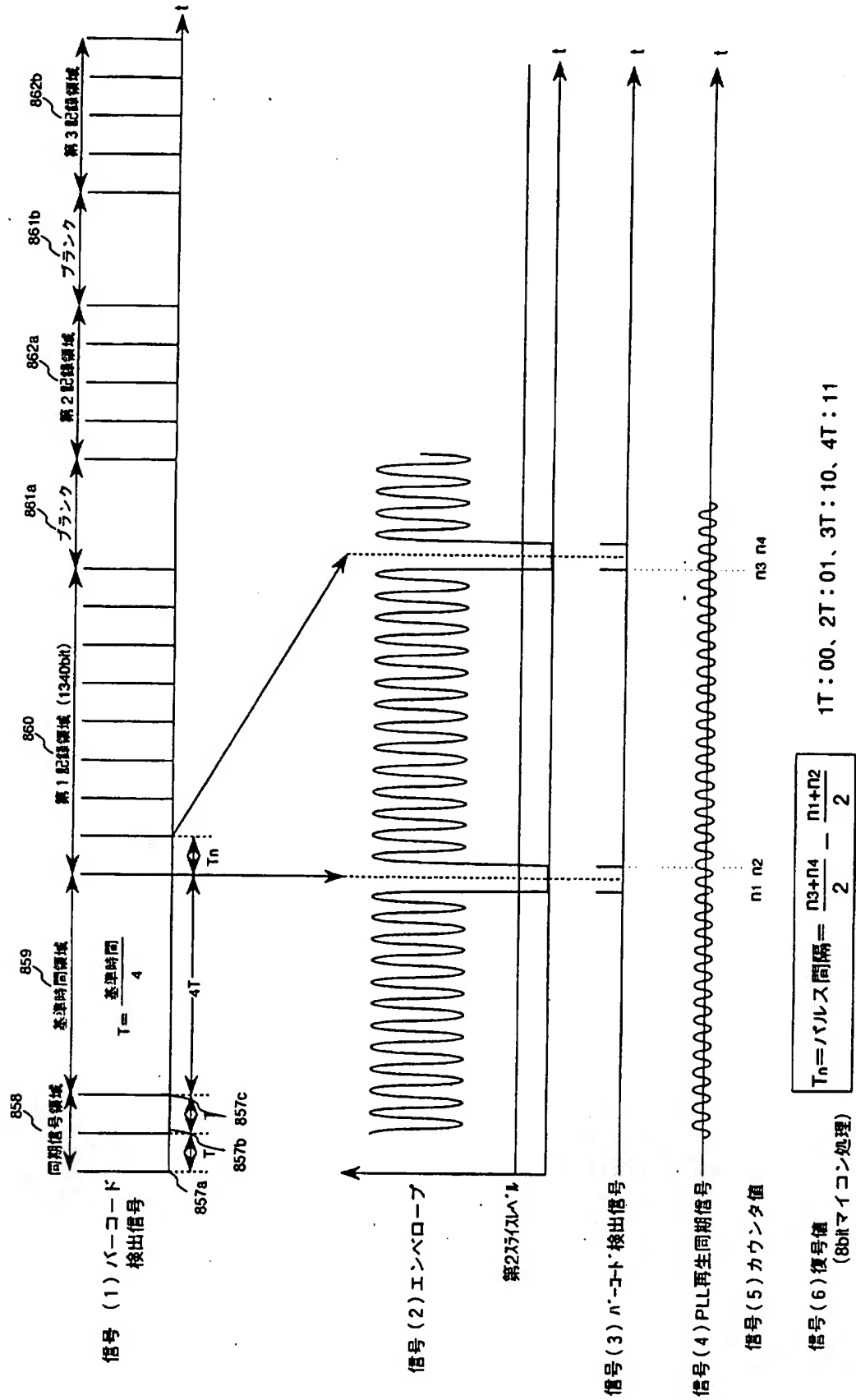
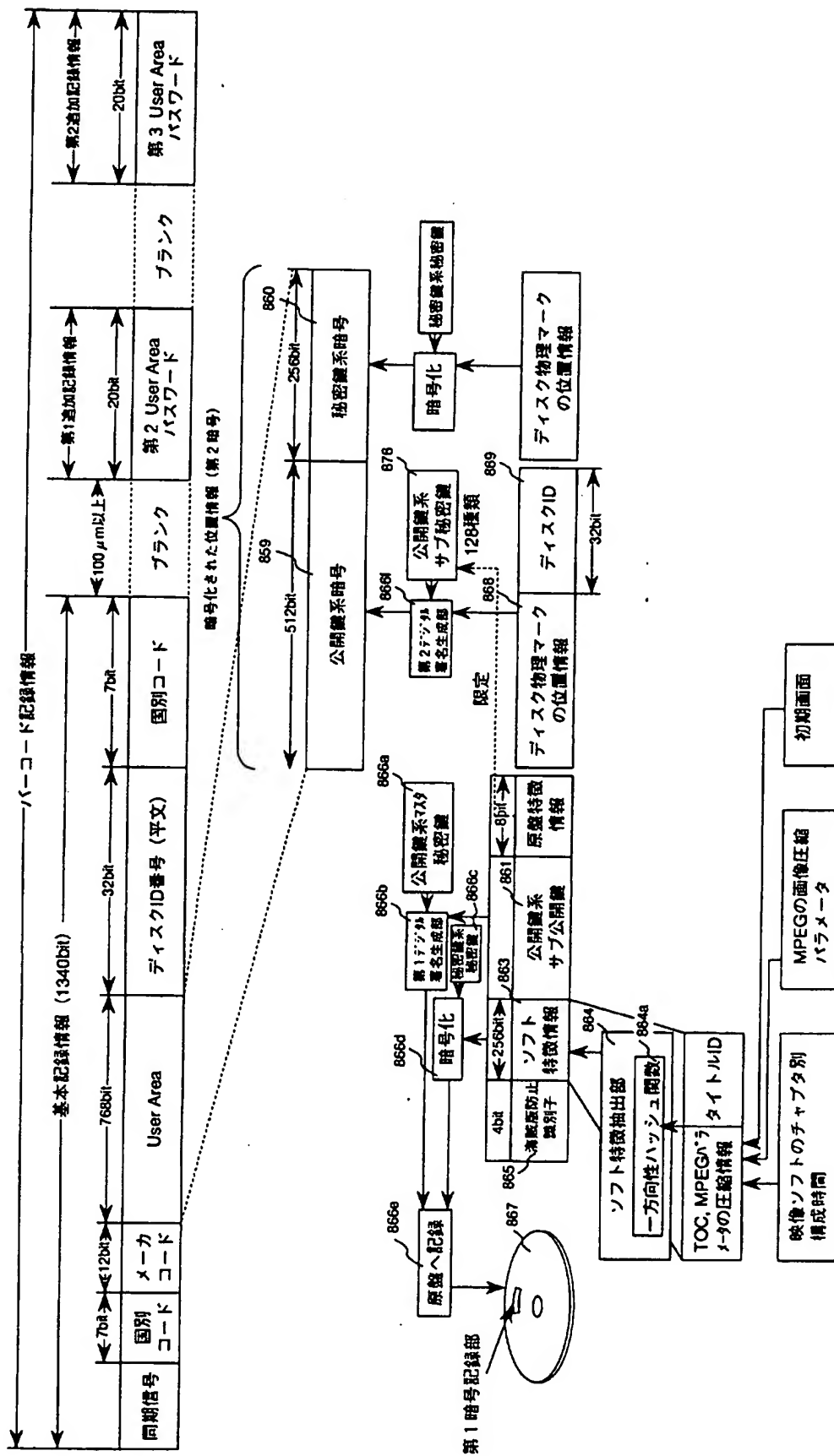


図 23 振



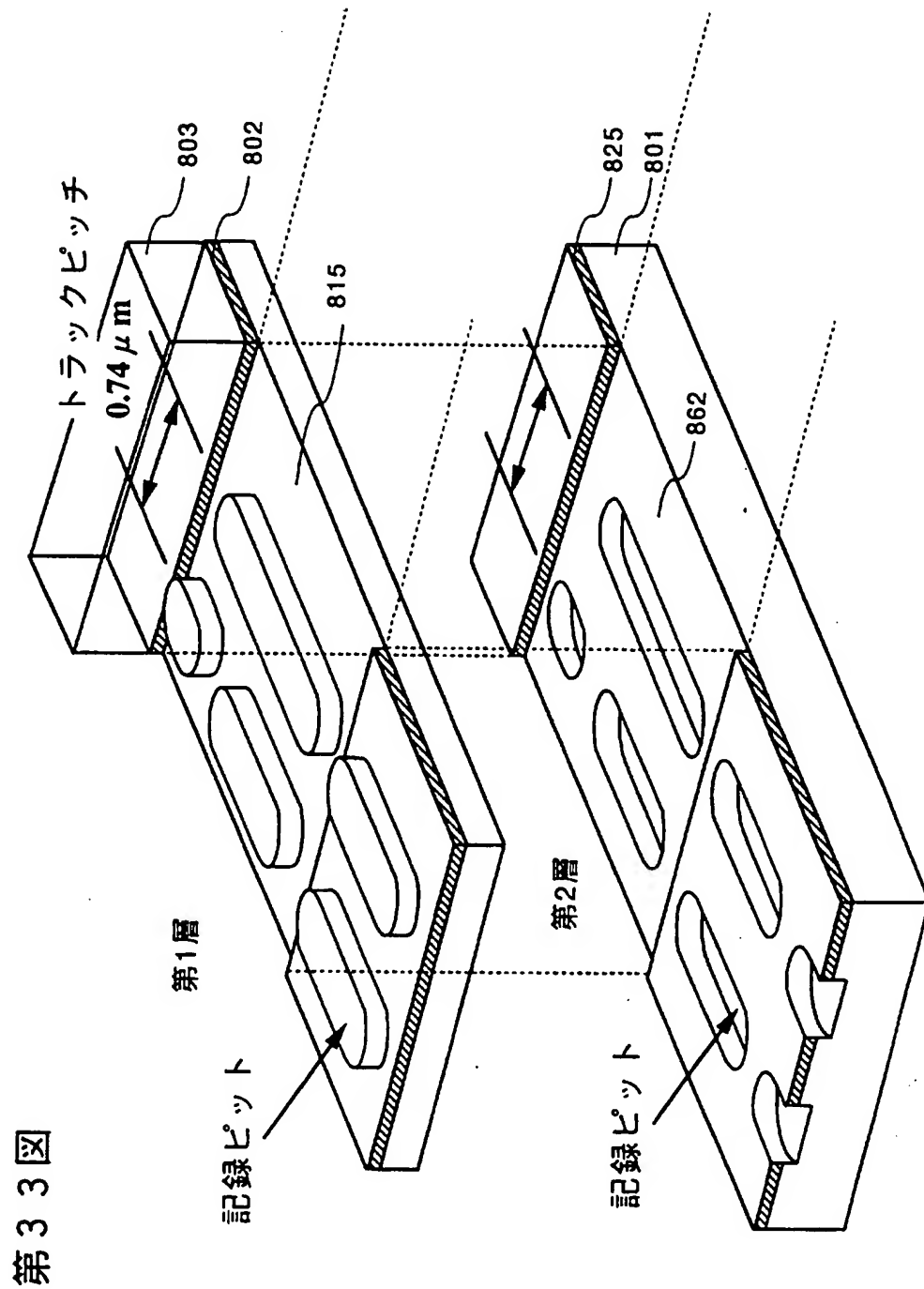
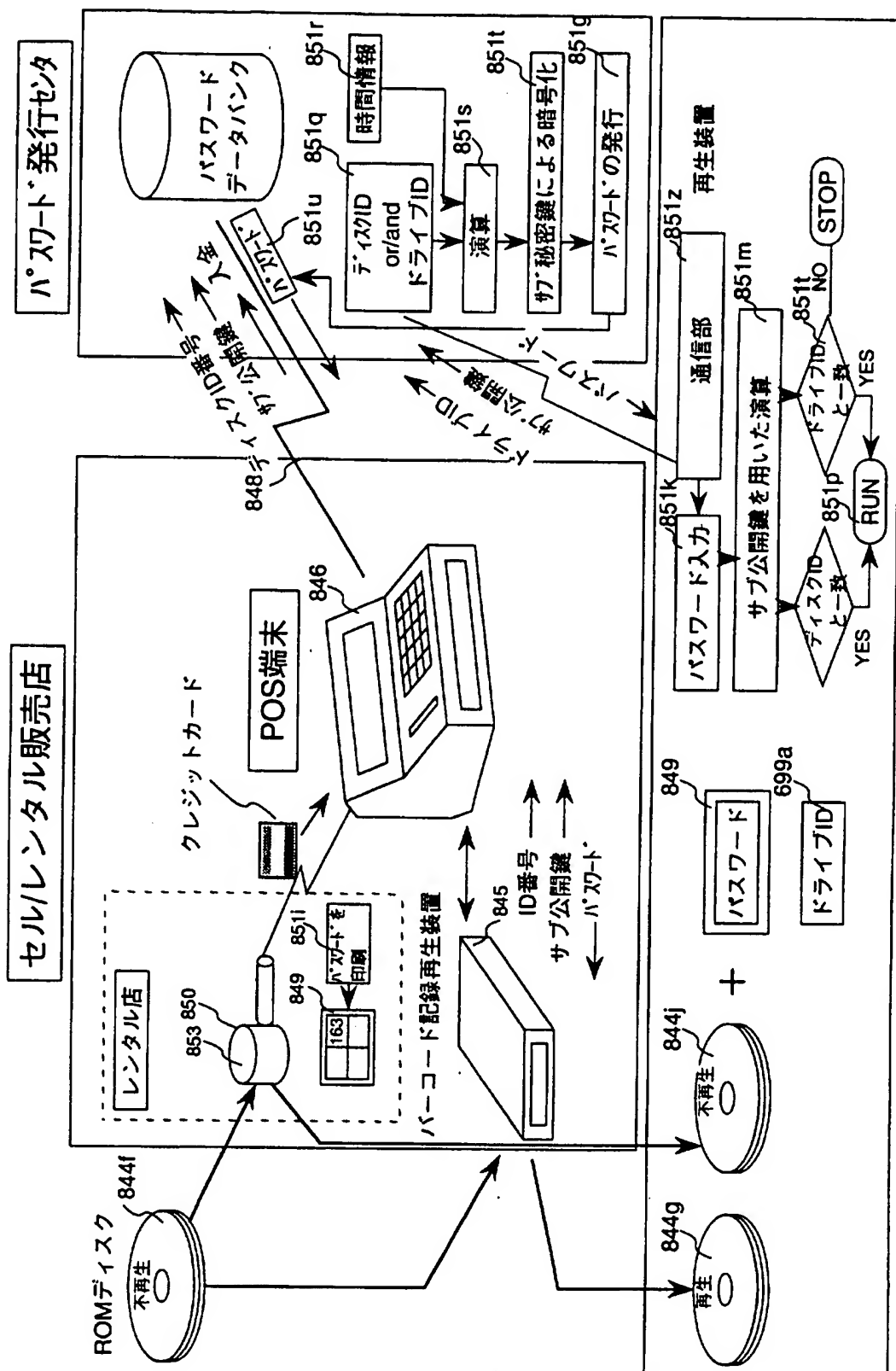
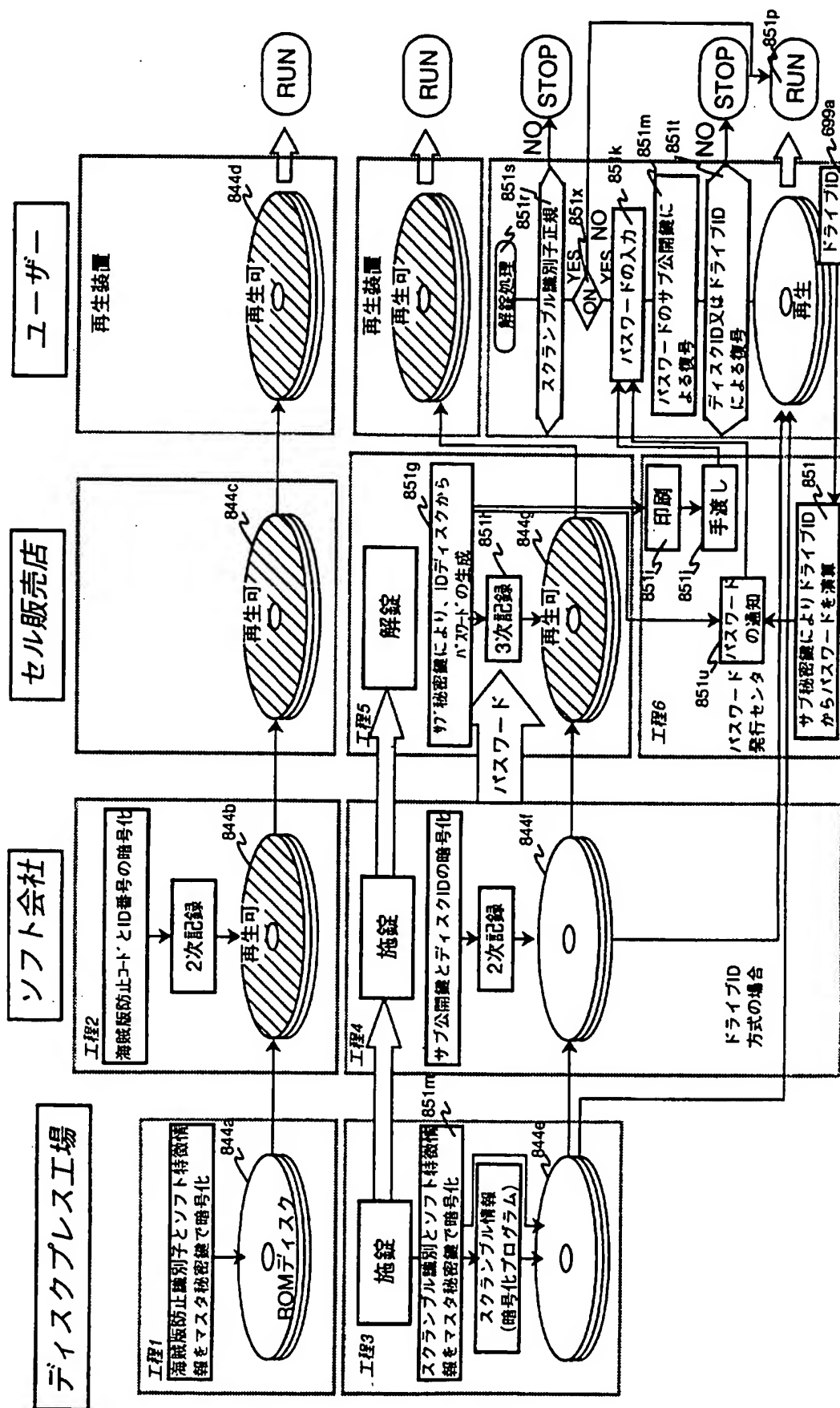


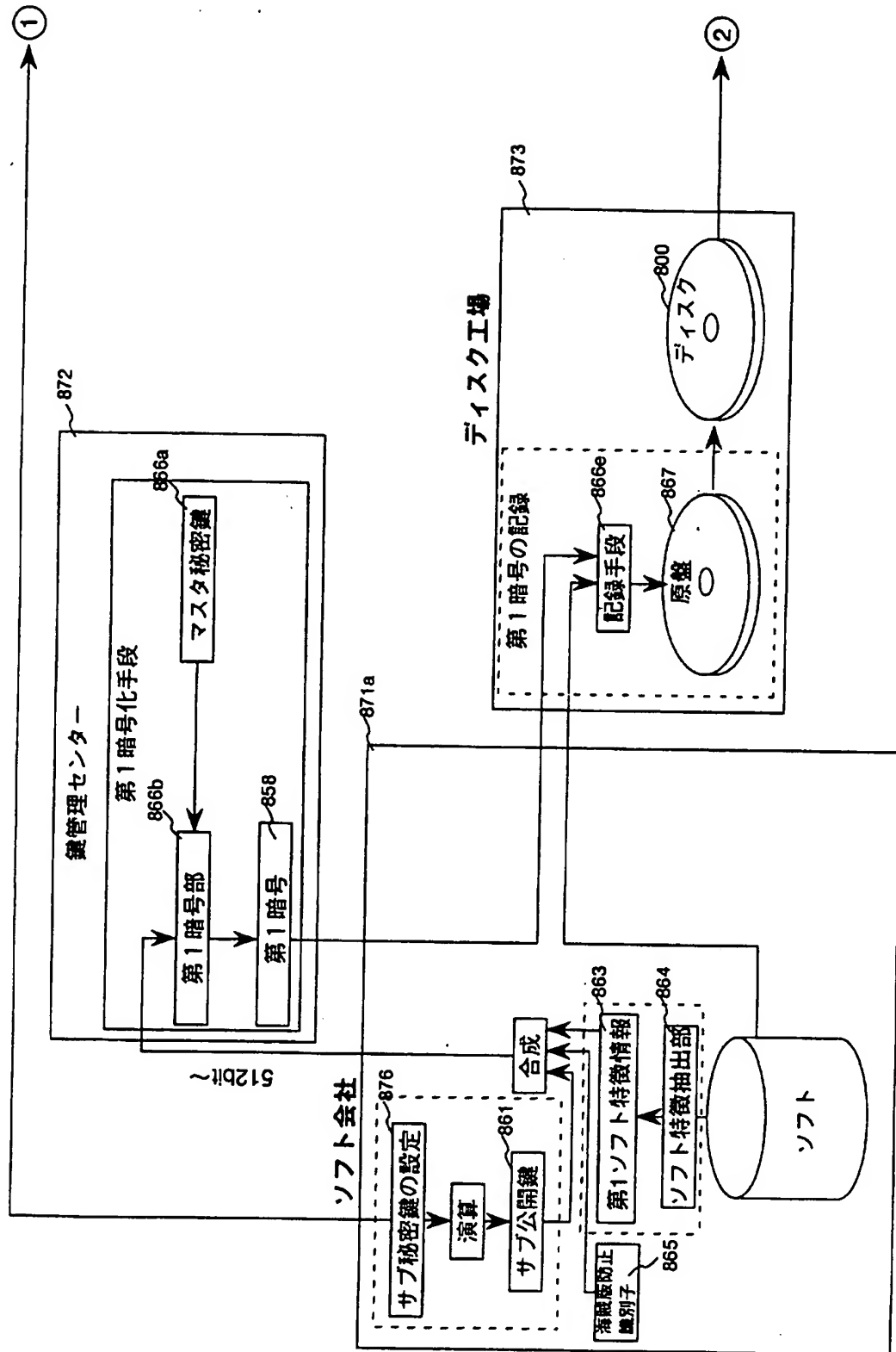
図 4 3 採



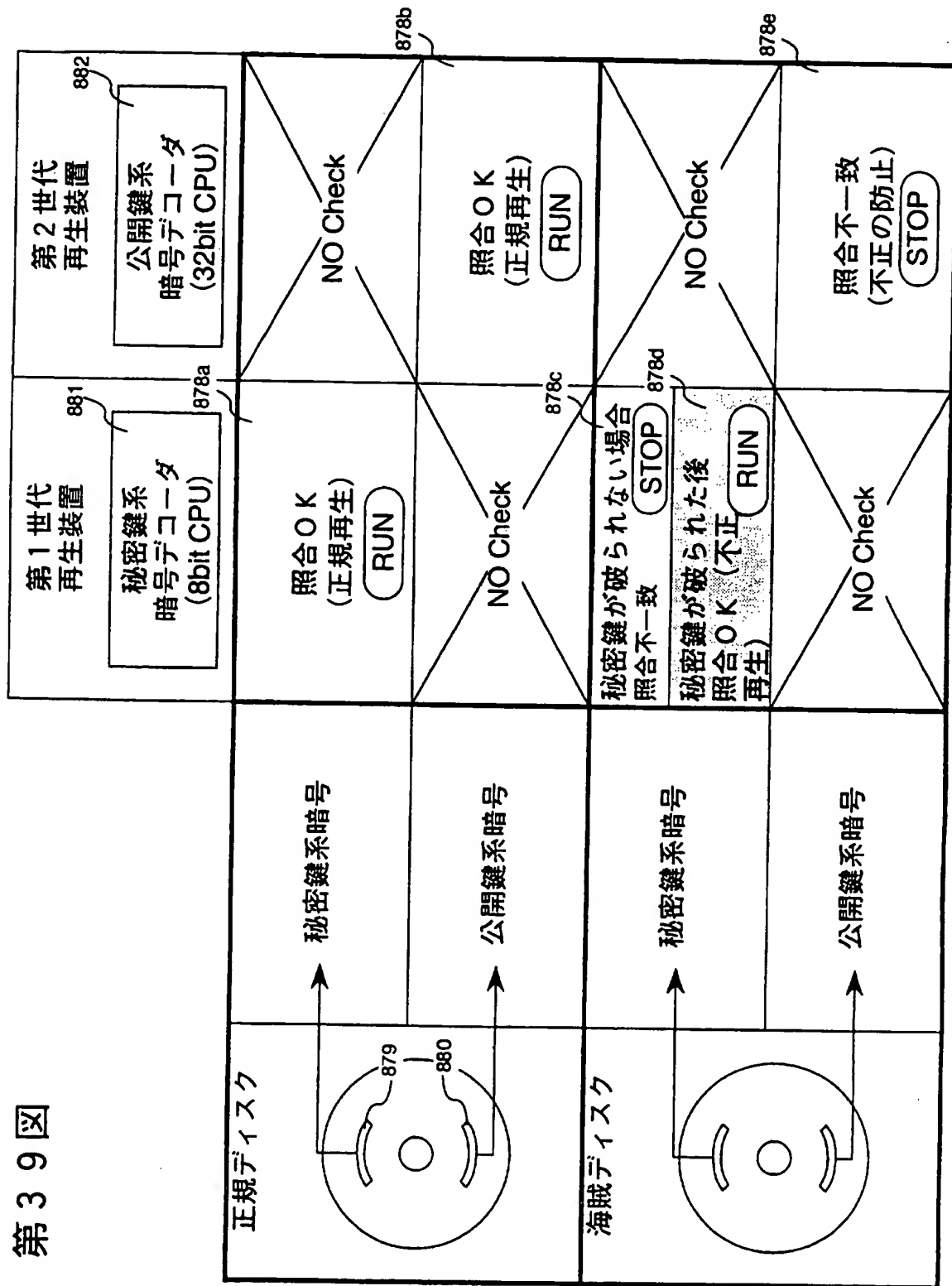
第 3 5 図



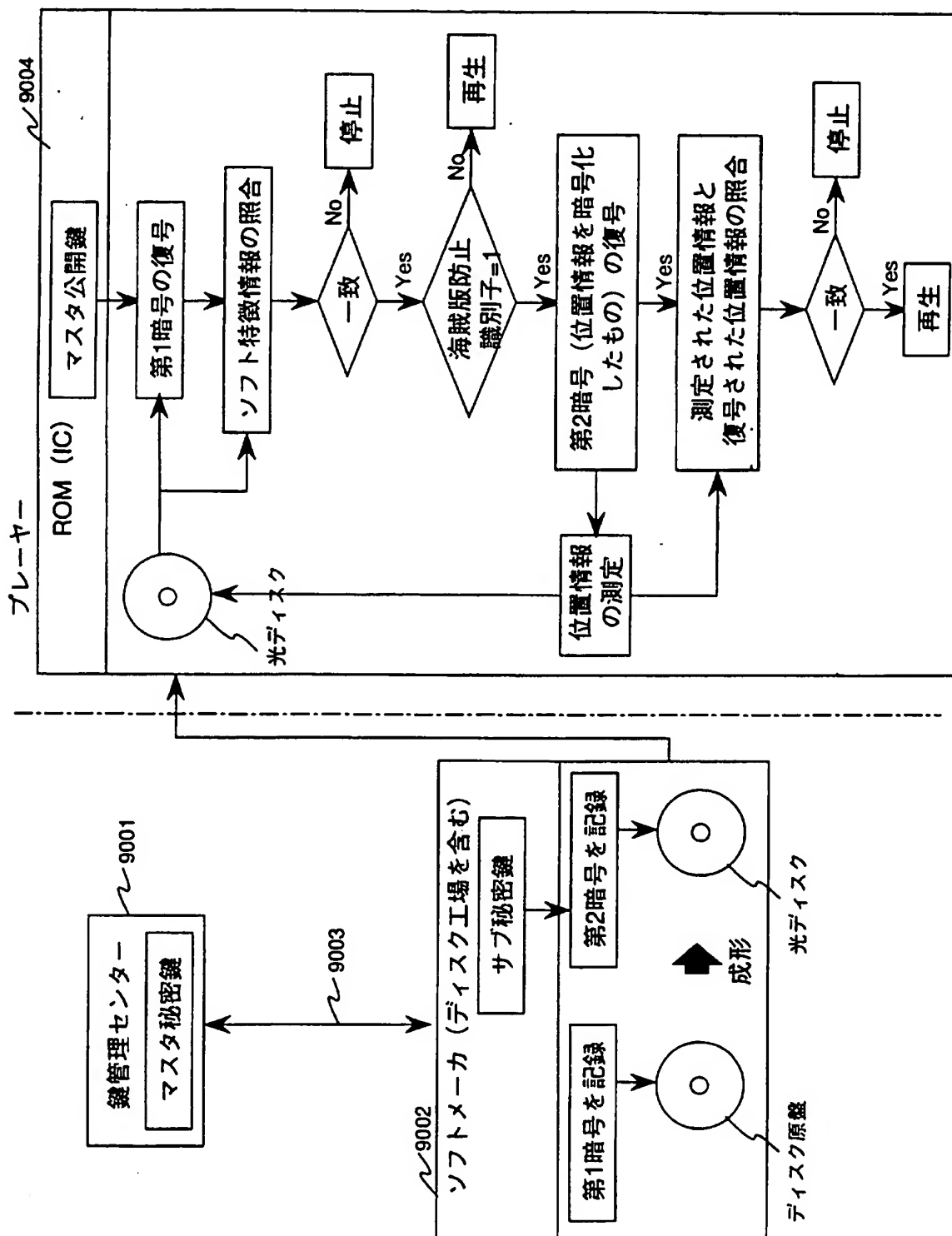
第36図



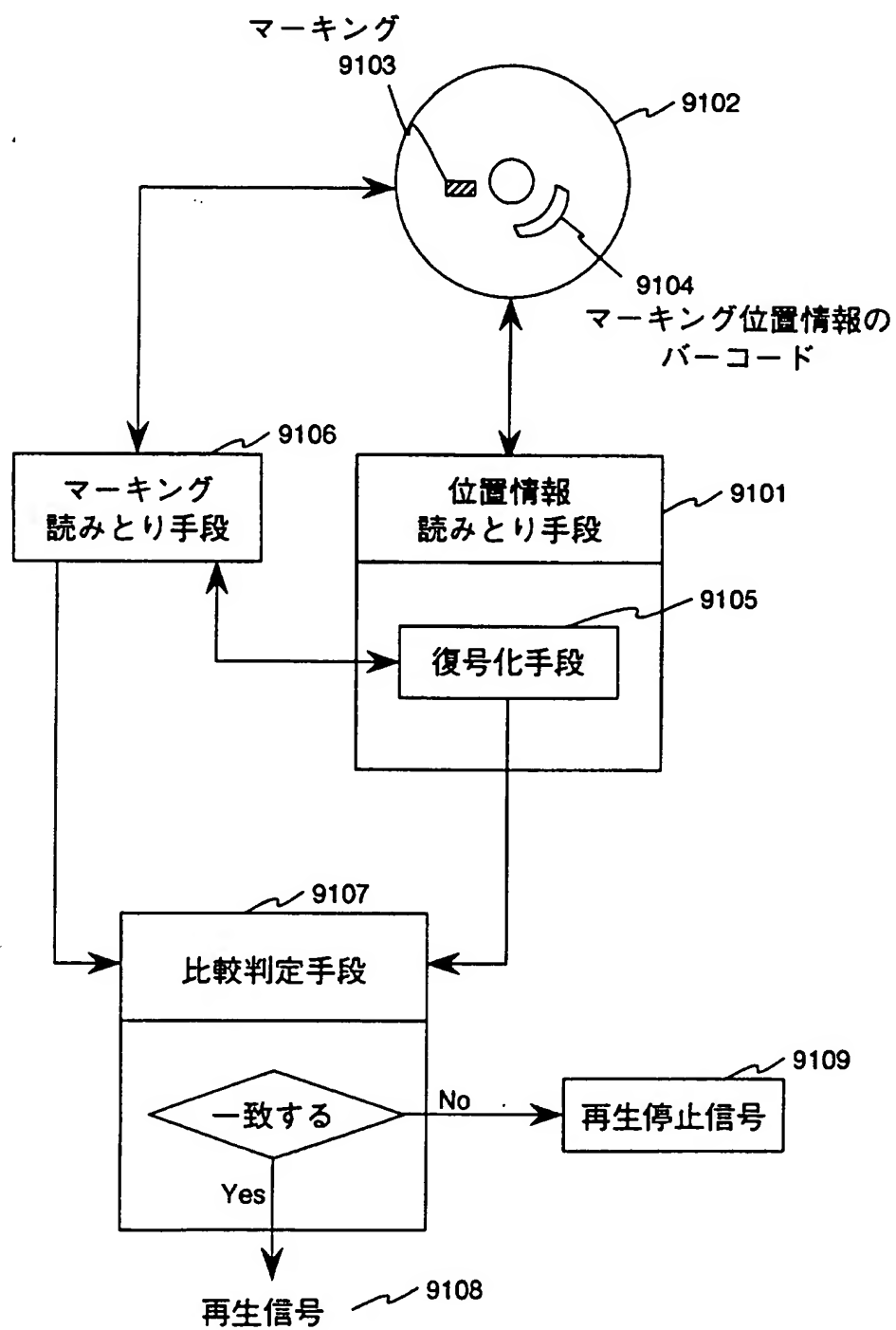
第 3 9 図



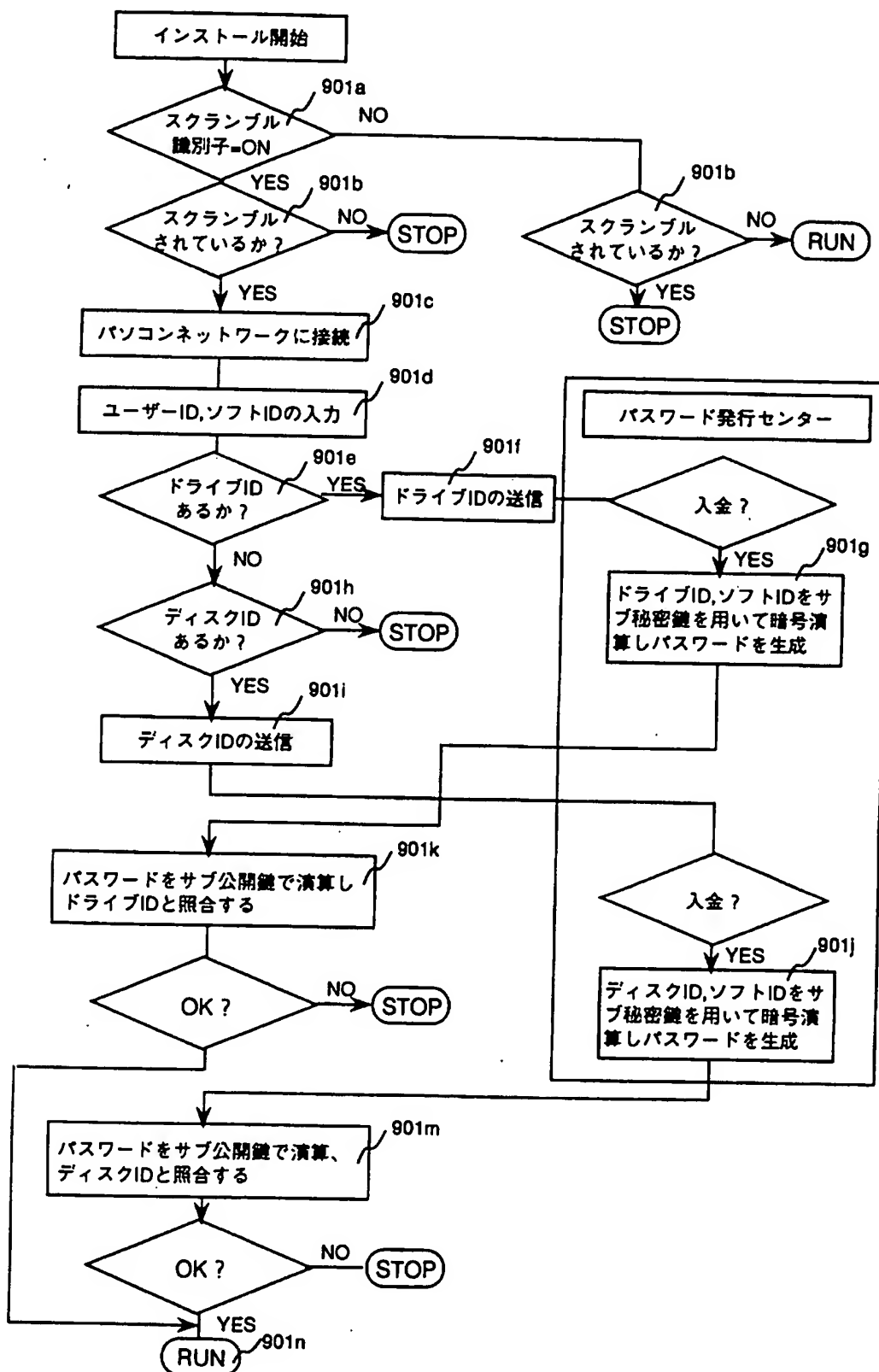
第40図



第 4 1 図



第 4 2 図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP95/02339

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl⁶ G11B7/00, G11B20/10, G11B7/26, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl⁶ G11B7/00, G11B20/10, G06F12/14, G11B7/26, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1955 - 1995

Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 5-266576, A (Fujitsu, Ltd.), October 15, 1993 (15. 10. 93) (Family: none)	1-2, 13-14 6, 15, 25, 27
T	JP, 7-325712, A (Oki Electric Industry Co., Ltd.), December 12, 1995 (12. 12. 95) (Family: none)	3-11, 13-22, 25, 27
A	JP, 2-44448, A (NEC Corp.), February 14, 1990 (14. 02. 90) (Family: none)	1-11, 13-22, 25
A	JP, 63-46541, A (NEC Corp.), February 27, 1988 (27. 02. 88) (Family: none)	5, 8, 17, 20
A	JP, 63-164043, A (Toshiba Corp.), July 7, 1988 (07. 07. 88) (Family: none)	11-12, 23-24
A	JP, 61-190734, A (Matsushita Electric Ind. Co., Ltd.), August 25, 1986 (25. 08. 86) (Family: none)	26

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
January 8, 1996 (08. 01. 96)

Date of mailing of the international search report
January 30, 1996 (30. 01. 96)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. G11B7/00, G11B20/10, G11B7/26,
G11B20/12

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. G11B7/00, G11B20/10, G06F12/14,
G11B7/26, G11B20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1955-1995年
日本国公開実用新案公報 1971-1995年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP, 5-266576, A (富士通株式会社), 15. 10月. 1993 (15. 10. 93) (ファミリーなし)	1-2, 13-14 6, 15, 25, 27
T	JP, 7-325712, A (沖電気工業株式会社), 12. 12月. 1995 (12. 12. 95) (ファミリーなし)	3-11, 13-22, 25, 27
A	JP, 2-44448, A (日本電気株式会社), 14. 2月. 1990 (14. 02. 90) (ファミリーなし)	1-11, 13-22, 25

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 先行文献ではあるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日
若しくは他の特別な理由を確立するために引用する文献
(理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願の日
の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と
矛盾するものではなく、発明の原理又は理論の理解のため
に引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規
性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文
献との、当業者にとって自明である組合せによって進歩性
がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

08. 01. 96

国際調査報告の発送日

30.01.96

名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号 100
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

井 上 信 一

5 D 9 4 6 4

電話番号 03-3581-1101 内線 3553

C (続き). 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 63-46541, A (日本電気株式会社), 27. 2月. 1988 (27. 02. 88) (ファミリーなし)	5, 8, 17, 20
A	JP, 63-164043, A (株式会社 東芝), 7. 7月. 1988 (07. 07. 88) (ファミリーなし)	11-12, 23-24
A	JP, 61-190734, A (松下電器産業株式会社), 25. 8月. 1986 (25. 08. 86) (ファミリーなし)	26

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.